Philipps Universität Marburg

Dienstanweisung zur Nutzung einer Software zum Endgeräteschutz bei dienstlich genutzten IT-Systemen

Stand: 02.01.2024, Version 1.2

Die Philipps-Universität weist Personen, die dienstlich ein IT-System (Rechner oder Server) nutzen darauf hin, dass, sofern keine geeignete Software zum Schutz des Systems eingesetzt wird, die Nutzung mit Sicherheitsrisiken verbunden ist, die die gesamte IT-Infrastruktur der Philipps-Universität gefährden können. Dies gilt insbesondere für Windows-Systeme, die sich im Active Directory der Philipps-Universität befinden.

Um einen sicheren Betrieb von Windows-Systemen zu gewährleisten, sind Sie als nutzende oder administrierende Person eines dienstlichen Windows-Systems zur Einhaltung der folgenden Regelungen verpflichtet.

1 Vorhandene Regelungen

Die Nutzung eines dienstlichen Windows-Systems unterliegt der Ordnung der Philipps-Universität für die Nutzung und den Betrieb der Informationstechnologie, der Informationssicherheitsleitlinie der Philipps-Universität sowie der Richtlinie zur Administration von IT-Systemen und IT-Diensten im Netzwerk der Philipps-Universität. Diese Dienstanweisung ist eine Konkretisierung von Absatz 4.1 der Richtlinie zur Administration von IT-Systemen und IT-Diensten und benennt eine geeignete Sicherheitslösung, die nutzende und administrierende Personen für dienstliche Windows-Rechner einsetzen müssen.

2 Regelungen für dienstliche Windows-Rechner

Ein dienstliches Windows-System ist ein Rechner, Laptop, virtueller oder physischer Server mit einem Windows-Betriebssystem, der im Wesentlichen für die Erfüllung dienstlicher Aufgaben genutzt wird und durch finanzielle Mittel der Philipps-Universität beschafft wurde. Für diese Systeme gelten die folgenden Regelungen:

1. Für das Windows-Betriebssystem müssen regelmäßig Sicherheitsupdates installiert werden. Dienstliche Windows-Systeme, die keine regelmäßigen Sicherheitsupdates mehr erhalten, dürfen nicht im universitären Netzwerk (LAN und WLAN) genutzt werden. Für diese Windows-Systeme gelten die nachfolgenden Regelungen nicht.
2. Auf allen dienstlichen Windows-Systemen, die sich im Active Directory der Philipps-Universität befinden, muss die vom Hochschulrechenzentrum zentral bereitgestellte Software[1] installiert und dauerhaft genutzt werden.
3. Auf allen dienstlichen Windows-Systemen, die sich nicht im Active Directory der Philipps-Universität befinden, kann nur in begründeten Ausnahmefällen auf die Nutzung der vom Hochschulrechenzentrum zentral bereitgestellten Software verzichtet werden. Ausnahmen müssen schriftlich per E-Mail an it-sicherheit@uni-marburg.de gemeldet werden.

3 Informationen zur vom Hochschulrechenzentrum zentral bereitgestellten Software zum Endgeräteschutz

Für an der Philipps Universität Marburg eingesetzte Windows-Systeme wird eine cloudbasierte Software zum Endgeräteschutz bereitgestellt:

[1] Zu finden unter https://www.uni-marburg.de/de/hrz/dienste/virenschutz.

- Auf vom Hochschulrechenzentrum per Opsi gemanageten Arbeitsplatzrechnern ist die Software standardmäßig installiert und wird automatisch regelmäßig aktualisiert.
- Der Einsatz ist ausschließlich für Dienstgeräte vorgesehen.
- Auf privat angeschafften Systemen ist die Nutzung auf Grund der zentralisierten Verwaltung nicht vorgesehen. Aktuelle Versionen von Microsoft Windows enthalten bereits einen funktionierenden Virenschutz (Windows Defender).

Marburg, 16.01.2024

gez. Prof. Dr. Thomas Nauss