Info für das Personal aus Forschung, Lehre und Verwaltung

Auf die PH wurde ein Cyberangriff durchgeführt, bei dem am Pfingstsamstag von den Angreifern u.a. die Daten auf unseren Servern verschlüsselt wurden. Die Auswirkung dieses Angriffs ist so gravierend, dass wir die gesamte IT-Infrastruktur neu aufbauen müssen. Derzeit geht es insbesondere darum, die Basisinfrastruktur (Campusnetz, Funknetz, Serverpark, …) neu aufzusetzen. Dies wird einige Zeit in Anspruch nehmen, ist aber Voraussetzung für die von Ihnen genutzten Dienste.

Es ist davon auszugehen, dass die Angreifer schon im Vorfeld länger im PH-Netz aktiv waren, so dass potenziell auf jedem Dienstrechner Schadsoftware vorhanden sein kann. Deshalb sollten Sie Ihre Dienstrechner aktuell nur offline verwenden. Beim Anschluss an einen Hotspot oder an Ihr Heimnetzwerk, an dem auch andere Geräte angeschlossen sind, sowie bei angeschlossenen externen Speichermedien besteht die Gefahr der Verschlüsselung für alle erreichbaren Geräte. Hingegen ist die Gefahr tolerierbar, wenn Sie als Einzelgerät ins Internet gehen (z.B. über ein Handy-Hotspot).

Wir werden nach und nach alle Dienstrechner mit Betriebssystem und Standardsoftware neu aufsetzen und den Virenschutz Bitdefender installieren. Ggf. auf den Rechnern vorhandene, lokale Daten werden wir sichern und können diese – nach einer Bereinigung – wieder zur Verfügung stellen.

Wir versuchen, den Zeitraum, im dem die Nutzer ohne Dienstgerät arbeiten müssen, zu minimieren. Zur Rückgabe der bereits abgegebenen Geräte werden wir umgehend informieren. Ebenso erfolgt eine Information wie weitere Abgaben optimal organisiert werden. Bis dahin können Sie mit den Geräten offline arbeiten.

Vor dem Gebrauch externer Speichermedien (USB-Sticks, Festplatten, …) müssen diese mit dem auf den neu aufgesetzten Rechnern installierten Bitdefender von Ihnen gescannt und ggf. vom ZIK bereinigt werden.

Sollten Sie bei Ihren nicht bereinigten Geräten Hinweise auf Schadsoftware feststellen (z.B. durch den vorhandenen Virenscanner), wenden Sie sich bitte an das Help-Desk.

Falls beim Scannen externer Speichermedien ein Befall von Dateien mit Schadsoftware erkannt wird, führen Sie bitte selbst keine Bereinigung durch, sondern geben die befallenen Speichermedien umgehend beim ZIK Helpdesk zur Forensik (Untersuchung) und zur Bereinigung und ggf. Sicherung nicht betroffener Dateien ab.

Für den Bereich der Verwaltung konnten wir einen aktuellen Stand der Daten auf den Netzlaufwerken sichern. Im Bereich Forschung und Lehre konnten wir bei den Home-Laufwerken (V:) den Stand bis kurz vor Pfingsten sicherstellen. Bei den Forschung-und-Lehre -Gruppenlaufwerken haben wir nach derzeitigem Kenntnisstand evtl. nur eine Datensicherung von vor 70 Tagen zur Verfügung. Diese Daten werden nach dem Neuaufbau der Infrastruktur wieder zur Verfügung gestellt werden können.

Es gilt allerdings: **Eine Verwendung der neu aufgesetzten Rechner im Hochschulnetz wird erst nach dem Neuaufbau der IT-Basisinfrastruktur möglich sein.**