Wichtige Informationen zum Thema Informationssicherheit

Aktueller Anlass:
In der **Hausdruckerei** wurden über einen ungekannten Zeitraum **Speichermedien von Kunden** mit **Schadcode** verseucht. Falls Sie in der letzten Zeit dort gedruckt haben, sollten sie die genutzten Datenträger nicht mehr an einen Computer ohne aktuellen und aktiven Virenschutz anschließen.

Wie können Sie sich und Ihre Kolleg*innen schützen?

- Schützen Sie mobile Datenträger (z.B. USB Sticks) und Ihr Laptop, vor unbefugtem Zugriff, Manipulation und Verlust. Bei Dienstreisen sollten Sie nicht unbeaufsichtigt gelassen werden. Wenn möglich sollten Daten verschlüsselt transportiert werden. Schließen Sie keine Datenträger an ein fremdes System an, um die Verbreitung von Schadsoftware zu verhindern.
  Mehr Informationen auf: https://hilfe.uni-paderborn.de/Daten_sicher_aufbewahren

- Prüfen Sie auch E-Mails von Ihnen bekannten Absendern kritisch. Stimmt die Sprache? Ist das Anliegen realistisch? Bevor Sie Links oder Anhänge öffnen: Fragen Sie im Zweifel in einer neuen E-Mail (nicht als Antwort auf die empfangene!) beim vermeintlichen Absender nach, ob er Ihnen tatsächlich etwas geschickt hat.
  Mehr Informationen auf: https://hilfe.uni-paderborn.de/Hinweise_zu_Phishing-E-Mails und https://hilfe.uni-paderborn.de/Signierte_E-Mails

- Halten Sie Betriebssystem, Virenschutzprogramm und Ihre anderen Programme immer aktuell. Neu erscheinende Updates sollten Sie so schnell wie möglich installieren. Computer mit Betriebssystemen, die nicht mehr mit Sicherheitsupdates versorgt werden, müssen vor den Zugriffen dritter geschützt werden. Ist eine Aktualisierung nicht möglich müssen individuelle Maßnahmen zum Schutz ergriffen werden.

  Neben Windows Defender bietet das IMT Sophos Antivirus an. Dieser Service ist für Mitarbeitende, Studierende und Bereiche der Universität Paderborn (Fakultäten, Institute, Professuren, Einrichtungen, Gremien, Hochschulgruppen) konzipiert und beinhaltet die Versorgung von Arbeitsplätzen mit aktueller Antivirensoftware manuell oder automatisch über bereitgestellte Update-Server.
  Mehr Informationen auf: https://hilfe.uni-paderborn.de/Antivirensoftware

  Windows XP (Die Belieferung mit Sicherheitsupdates wurde im April 2014 eingestellt), Windows Vista (Die Belieferung mit Sicherheitsupdates wurde im April 2017 eingestellt) und Windows 7 (Die Belieferung mit Sicherheitsupdates wurde im Januar 2020 eingestellt) sollten nicht mehr ans Netzwerk der Hochschule angeschlossen werden.

  Auch Betriebssysteme wie Mac OS X und Linux müssen aktuell gehalten werden. Das gilt auch für mobile Betriebssysteme wie z.B. IOS und Android. Wer diese Systeme ohne weitere Sicherheitsmaßnahmen weiterhin betreibt, handelt grob fahrlässig.

- Sichern Sie Ihr System regelmäßig. Besitzen Sie ein Backup, lässt sich Ihr PC viel leichter wieder so herstellen, wie Sie ihn kennen und Daten – selbst wenn sie gelöscht oder verschlüsselt werden – können restauriert werden. Die Backups sollten getrennt von den Systemen gespeichert werden. Empfehlenswert ist es, Backups physisch und ohne Anbindung ans Internet an einem sicheren externen Ort aufzubewahren. Wichtige Passwörter sollten nicht nur digital, sondern auch in Papierform, sicher verschlossen, aufbewahrt werden.
  Mehr Informationen auf: https://hilfe.uni-paderborn.de/Datensicherung

- Arbeiten Sie bei den täglichen Dingen nicht mit Administrator-Rechten. Legen Sie bei Ihrem Betriebssystem ein Nutzerkonto ohne Administrator-Rechte an und arbeiten Sie nur damit. So kann keine Software ohne Rückfrage durch das Betriebssystem installiert werden.

- Schalten Sie Makros in Office-Programmen ab. Schädliche Software wird oft auf diesem Weg auf Computer geschleust. Sofern Sie nicht zwingend mit Makros in Ihrer Büro-Software arbeiten müssen, schalten Sie sie gänzlich ab.

Was ist zu tun, wenn Sie betroffen sind?

- Informieren Sie das Informationssicherheitsteam (informationssicherheit@uni-paderborn.de) und Ihr Umfeld über den Sachverhalt.
  Mehr Informationen auf: https://www.uni-paderborn.de/universitaet/informationssicherheit

- Ändern Sie alle auf den betroffenen Systemen gespeicherten und eingegebenen Zugangsdaten.

- Schadprogramme nehmen teilweise tiefgreifende (sicherheitsrelevante) Änderungen am infizierten System vor. Nach einer forensischen Sichtung müssen Sie diesen Rechner neu aufzusetzen oder neu aufsetzen lassen.

Brauchen Sie Hilfe?
Wenden Sie sich an den IT-Betrieb ihrer Fakultät.

Fakultät für Kulturwissenschaften
IT-Support für Mitarbeiter*innen der KW
https://kw.uni-paderborn.de/fakultaet/it-support

Fakultät für Wirtschaftswissenschaften
IT-Administration der Fakultät für Wirtschaftswissenschaften
https://wiwi.uni-paderborn.de/fakultaet/organisation/fakultaetsverwaltung

Fakultät für Naturwissenschaften

IT und IT-Sicherheit Fakultät für Naturwissenschaften
https://nw.uni-paderborn.de/fakultaet/organisation/it-und-it-sicherheit

Fakultät für Maschinenbau
MB IT
https://mb.uni-paderborn.de/mb-it

Fakultät für Elektrotechnik, Informatik und Mathematik
Informatik Rechnerbetrieb
https://cs.uni-paderborn.de/irb
Rechnerbetrieb Mathematik
https://math.uni-paderborn.de/rechnerbetrieb

Melden Sie sich bei Fragen zu Software oder zu Diensten des IMT beim Benutzerservice des IMT (imt@upb.de).

Haben Sie Fragen oder Anregungen zu den Themen Informationssicherheit? Zögern Sie nicht, sich beim Informationssicherheits-Team (informationssicherheit@uni-paderborn.de) zu melden.