Checkliste zur Grundsicherung von Computern und digitalen Daten

Details zur Umsetzung der Maßnahmen unter: http://www.itsb.rub.de/pcgrundsicherung.html

Basissicherung

1. Arbeiten mit mehreren passwortgeschützten Benutzerkonten

- ❒ Hat jeder Nutzer ein eigenes Benutzerkonto?
- ❒ Nutzen Sie ein eingeschränktes Benutzerkonto für das Internet?
- ❒ Werden von allen Nutzern sichere Kennwörter verwendet (mind. 8 Zeichen, Ziffern, Sonderzeichen sowie Groß- und Kleinschreibung, keine gebräuchlichen Begriffe oder Namen)?
- ❒ Erneuern Sie regelmäßig Ihre Passwörter?

2. regelmäßige Durchführung von Windows-Updates

- ❒ Wird das Betriebssystem über das Windows Update oder den Windows Update Server der RUB regelmäßig (halb-)automatisch aktualisiert (siehe http://windowsupdate.microsoft.com oder http://www.rz.ruhr-uni-bochum.de/dienste/software/sus/)?
- ❒ Werden andere Softwareprodukte (vor allem die mit Internetverbindung) regelmäßig aktualisiert?

3. Installation von Firewall und Antivirensoftware

- ❒ Ist eine Firewall aktiv? (Windows eigene Firewall oder Sophos)
- ❒ Ist eine Antivirensoftware installiert (z.B. Sophos als Campuslizenz)?
- ❒ Wird die Antivirensoftware regelmäßig aktualisiert?

4. regelmäßige Sicherung der Datenbestände (Backup)

- ❒ Werden die Datenbestände regelmäßig gesichert?
- ❒ Werden die Sicherungsmedien gesichert aufbewahrt?

5. Websurfen mit Sicherheitsbewusstsein

- ❒ Sind an Webbrowsern alle relevanten Sicherheitseinstellungen vorgenommen worden?

Organisatorische Sicherung

6. verantwortungsbewusster Umgang mit Chipkarten

- ❒ Bewahren Sie die Karte so auf, dass niemand Sie unbemerkt entnehmen oder „ausleihen“ kann.
- ❒ Ziehen Sie beim Verlassen des Arbeitsplatzes die Karte aus dem Kartenleser und nehmen sie mit.
- ❒ Ist die PIN sicher? (keine simple Ziffernfolgen, nicht das eigene Geburtsdatum etc.)
- ❒ Sind erforderliche Vertretungsregelungen eingerichtet?

Einen Kartenverlust melden Sie bitte umgehend unter: 32 - 23333. Die Karte wird dann gesperrt.

7. Zugänglichkeit der Geräte

- ❒ Ist klar, wer Zutritt zu Ihren Räumen hat? Sind das nur Berechtigte?
- ❒ Schließen Sie die Räume in Abwesenheit immer ab?
- ❒ Ist sichergestellt, dass sich Besucher nur in Ihrem oder im Beisein eines anderen Mitarbeiters im Büro aufhalten.
- ❒ Ist der Monitor so aufgestellt, dass niemand versehentlich Einsicht in Ihren Bildschirm nehmen kann?
- ❒ Sperren Sie den Rechner, wenn Sie den Arbeitsplatz verlassen? Windowstaste-L (ab Windows XP), Ctrl-Alt-Entf – Sperren.
- ❒ Ist ein Bildschirmschoner eingerichtet und muss bei Wiederinbetriebnahme das Passwort eingegeben werden.
- ❒ Ist der Rechner mit einem Schloss versehen?

8. Wartung und Entsorgung

- ❒ Werden Festplatten und Datenträger sicher entsorgt und sind sicher gelöscht, bevor sie weitergegeben werden?
- ❒ Werden Festplatten mit schützenswertem Inhalt auch bei Defekten nicht aus der Hand gegeben?

9. Privatnutzung

- ❒ Werden durch die private Nutzung von Geräten und Diensten dienstliche Belange nicht tangiert?
- ❒ Werden auch Privatgeräte in der RUB über den HIRN-Port in Betrieb genommen?

Erweiterte Sicherung

10. Datei-, Ordner- und Festplattenverschlüsselung

- ❒ Wissen Sie, wie man eine einzelne Datei verschlüsselt?
- ❒ Ist ein Ordner, der vertrauliche Informationen enthält verschlüsselt?
- ❒ Wenn auf Ihrem Rechner an vielen Stellen vertrauliche Daten gespeichert sind, ist die gesamte Festplatte verschlüsselt?
- ❒ Haben Sie bei der der Verschlüsselung sichergestellt, dass kein Passwort und Sicherheitsschlüssel/Zertifikat verloren geht? (Kopie des Passwortes im Umschlag im Tresor)

11. Überprüfung von Sicherheitslücken

- ❒ Ist der Rechner mit dem Baseline Security Analyzer überprüft worden?
- ❒ Sind alle gefundenen Probleme behoben?

Sie benötigen Hilfestellung?

Falls Sie mit den Maßnahmen zur Sicherung Ihres PCs nicht alleine zurecht kommen, hilft Ihnen das Servicecenter des Rechenzentrums gerne weiter. Auf Wunsch und gegen Kostenberechnung hilft Ihnen ein Mitarbeiter des Servicecenters auch auf dem Campus vor Ort bei der Absicherung Ihres PCs.

Weitere Informationen erhalten Sie online unter: http://www.rz.rub.de/kontakte/servicecenter/