DATENSCHUTZ-BEAUFTRAGTER DSB

Stabsstelle für Informationssicherheit

RUHR UNIVERSITÄT BOCHUM RUB 50 Jahre

Checkliste zur Grundsicherung von Computer 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 Intermet?
- ☐ Werden von allen Nutzern sichere Kennwörter verwendet (mind. 8 Zeichen, Ziffern, Sonderzeichen sowie Groß- und Kleinschreibung, keine gebräuchlichen Begriffen 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 Firewal 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?sind an Webbrowsern alle relevanten

5. Websurfen mit Sicherheitsbewusstsein

- ☐ Sicherheitseinstellungen vorgenommen worden?

Organisatorische Sicherung

6. Verantwortungsbewusster Umgang mit Chipkrten

- ☐ Bewahren Sie die Karte so auf, dass niemand Sie unbemerkt entnehmen oder „ausleihen“ kann.
- ☐ Ziehen Sie beim Verlassen des Arbeitsplätzes die Karte aus dem Kartenleser und nehmen Sie mit.
- ☐ Ist die PIN sicher? (keine simple Zifferfolgen, nicht das eigene Geburtsdatum etc.)

Einen Karteverlust 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 Räumen in Anwesendheit 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 viele Stellen vertrauliche Daten gespeichert sind, ist die gesamte Festplatte verschlüsselt?

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 gerne weiter.