Daher einige Grundregeln in der täglichen Arbeit:

- Wenn Sie Mails von unbekannten Adressen oder in dubioser Konstellation erhalten, verwerfen Sie diese.
- Ihr Systemadministrator oder die IT-Abteilung wird niemals die Übermittlung Ihres Passwortes oder Pin-Codes verlangen.
- Verwenden Sie die digitale Signatur zur Absicherung Ihres Dokumentenaustausches (z. B. mit der PDF-Signatur auch mit Handy).
- Öffnen Sie nicht automatisch alles, was Ihnen zugesandt wird, insbesondere keine unerwarteten E-Mails, die in einer unüblichen Sprache verfasst sind und von Unbekannten stammen. Dateianhänge von derartigen Absendern könnten mit Viren oder anderer Schadsoftware behaftet sein.
- Klicken Sie nicht willkürlich beim Surfen im Internet auf jegliches Angebot und prüfen Sie, bevor Sie Webseiten aufrufen, ob das Ihren Intentionen entspricht.
- Achten Sie beim Nutzen eines Angebotes im Internet, bei welchem sensible Daten eingegeben werden, dass Sie eine »sichere Verbindung« haben (meist Anzeige eines Schlosses im Browser).
- Achten Sie beim Herunterladen besonders auf Dateien, die für Sie unbekannte Endungen (also nicht .doc, .xls, usw.) aufweisen.
- Wenn Sie im Rahmen des Herunterladens zur Installation von Software aufgefordert werden, verständigen Sie sofort Ihre Hotline.

Abschließend sei angemerkt, dass absolute Sicherheit in der virtuellen Welt nicht möglich ist. Mit der Einhaltung einiger Grundverhaltensregeln wird es aber jenen, die versuchen, unbefugt an Informationen zu gelangen, erschwert, diese zu bekommen.

Mit der Berücksichtigung einiger weniger Maßnahmen aus diesem Folder sind wir **sicher,** dass Sie mithelfen, **sicher** zu sein.

Sollte es trotz Berücksichtigung der angeführten Punkte zu einem Vorfall kommen, dann wenden Sie sich umgehend an die IT-Hotline Ihrer Organisation. Wenn das Problem über Ihre Organisation hinaus geht und die öffentliche Verwaltung betrifft, steht Ihnen das GovCERT-Team unter folgenden Kontakten zur Verfügung:

- E-Mail: team@govcert.gv.at oder
- Telefonisch: +43 1 5056416 78 erreichbar von Montag bis Freitag (an Werktagen, ausgenommen 24. und 31. Dezember), jeweils von 8 bis 18 Uhr.

Sind Sie sicher?

Informationssicherheit in der öffentlichen Verwaltung

Impressum
Medieninhaber und Herausgeber: Bundeskanzleramt Österreich, GovCERT
Ballhausplatz 2, 1014 Wien, www.govcert.gv.at;
Grafische Gestaltung: ARGE Grafik; Druck: BM.I Digitalprintcenter; Wien, 2011

Laufend kommt es zu Sicherheitsvorfällen, diese zeigen uns sehr beeindruckend, wie schnell sensible Daten der öffentlichen Verwaltung in falsche Hände geraten können. Oftmals sind es nur Kleinigkeiten, die man zu beachten hat, um derartig unerwünschte Offenlegungen von Daten bzw. Zugängen zu Systemen besser abzusichern.

Nachfolgend findet sich ein Überblick über Möglichkeiten der Absicherung auf einfache Art und Weise.

Verantwortung trifft uns »ALLE«

Jede Mitarbeiterin und jeder Mitarbeiter sowie Führungskräfte der öffentlichen Verwaltung müssen in ihrem Arbeitsumfeld darauf achten, dass die Sicherheitsmaßnahmen und -regelungen eingehalten werden. Nur eine breite Umsetzung des Sicherheitsbewusstseins im Arbeitsalltag kann uns vor möglichen unangenehmen Folgen schützen.

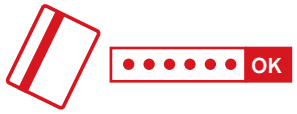
Nachfolgend einige Grundregeln im alltäglichen Verhalten am Arbeitsplatz:

- Wenn Sie den PC-Arbeitsplatz verlassen, sperren Sie diesen mittels Bildschirmschoner.
- Lassen Sie wichtige Unterlagen weder am Schreibtisch noch elektronisch am PC oder nach Besprechungen offen liegen, sondern versperren diese (Schreibtischlade oder PC-Sperre) bzw. nehmen Sie sie in Ihr Büro zurück.
- Überlegen Sie sich bei Dokumenten und Informationen, die Sie erstellen oder bearbeiten, ob diese einer nationalen oder internationalen Klassifikation (eingeschränkt, vertraulich usw.) unterliegen. Je nach Klassifikation behandeln Sie die Schriftstücke entsprechend.
- Versenden Sie klassifizierte Dokumente niemals über das offene Internet ohne zusätzlichen Schutz. Verwenden Sie sichere Anwendungen, wie das Elektronische Aktensystem oder die Verschlüsselung Ihrer Bürgerkarte und vergewissern Sie sich, welche Schutzmaßnahmen für die entsprechende Klassifizierungsstufe einzuhalten sind.
- Wenn Sie unterwegs sind, achten Sie darauf, dass vertrauliche Informationen nicht auf Ihrem Notebook ungeschützt verfügbar sind.
- Verwenden Sie nicht das gleiche Passwort im Dienstbereich wie auch im privaten Bereich, z.B. bei Google, Facebook, Twitter usw.
- Wenn Sie Verdacht schöpfen, setzen Sie sich unmittelbar mit Ihrer Hotline in Verbindung.
- Berücksichtigen Sie die von Ihrem Informationssicherheitsbeauftragten vorgegebenen Maßnahmen, auch wenn diese manchmal unpraktisch bzw. nicht sehr bequem sind.

Zugangsinformationen, Passwort, UserID und Zugangskarte

Passwörter und Pin-Codes von Zugangskarten bzw. Bürgerkarten sind der Schlüssel zu unseren Informationssystemen (wie auch der Schlüssel in Ihr Büro) und stellen damit einen besonderen Wert dar. Besondere Sicherheit stellen Zugangsmechanismen mit zwei Komponenten dar, nämlich Wissen (Passwort oder Pin-Code) und Besitz (Karte), wie es die Bürgerkarte umsetzt. Bei der Verwendung von ausschließlich Benutzerkennung und Passwort besteht die Gefahr, dass diese Hackern in die Hände fallen. Mit einigen Maßnahmen können aber auch Passwörter entsprechend abgesichert werden.

Daher wäre Folgendes zu beachten:



- Passwörter sind in regelmäßigen Abständen zu ändern.
- Passwörter dürfen auf keinen Fall weitergegeben werden.
- Wenn Sie den Verdacht haben, dass Ihr Passwort einem Dritten bekannt ist, ändern Sie es umgehend.
- Schreiben Sie Passwörter nirgends auf, versperren Sie diese eventuell auch in einem elektronischen Passworttresor.
- Verwenden Sie nicht das gleiche Passwort in der Behörde wie auch bei privaten Anbietern, wie Facebook, Google, Hotmail, usw.
- Es gilt das Grundprinzip: Das Passwort muss für Sie leicht merkbar, aber für andere schwer erratbar bzw. aufgrund seiner Merkmale nicht ableitbar (z.B. Geburtsdatum) sein.
- Verwenden Sie bei der Gestaltung des Passwortes immer eine Kombination aus Buchstaben, Zahlen und Sonderzeichen.

Auch außerhalb des Büros sicher

Wenn Sie Informationen außerhalb des Büros bzw. unterwegs verwenden, achten Sie besonders darauf, dass diese Informationen gut abgesichert sind und nicht leicht zugreifbar.

Hier einige Grundregeln:

- Nehmen Sie nur jene Daten mit, die Sie auch tatsächlich benötigen.
- Achten Sie bei der Verwendung des Notebooks, Tablets, Smartphones, usw. in öffentlichen Bereichen (Flughafen, usw.), dass niemand Ihre vertraulichen Informationen mitliest.
- Auf Dienstreisen mittels Flug oder Bahn behalten Sie Notebook, Tablet, Handy, Smartphone, Datenstick, usw. immer im Handgepäck.
- Beachten Sie, dass vertrauliche Informationen, auch wenn sie am Notebook abgespeichert sind, in einem sicheren Bereich bzw. verschlüsselt abgelegt werden.
- Lassen Sie Notebook, Tablet, Handy, Smartphone, Datenstick, usw. nicht sichtbar z.B. im Auto oder in anderen Bereichen liegen.
- Achten Sie bei Ihrem Notebook auf einen aktuellen Virenscanner.

Sichere E-Mail-Kommunikation und sicher im Internet

Computerviren und andere Schadsoftware werden meist über das Internet beim Surfen bzw. über E-Mail verteilt. Grundsätzlich sind die Systeme der öffentlichen Verwaltung gut abgeschirmt und mit sogenannten Virenscannern ausgestattet. Dennoch kann es vorkommen, dass Schadsoftware Ihren PC oder Ihr Notebook verseucht.