BMBWF
BUNDESMINISTERIUM
FÜR BILDUNG, WISSENSCHAFT
UND FORSCHUNG

efit 21 digitale bildung

Sind Sie sicher?

Informationssicherheit in der öffentlichen Verwaltung

Impressum

Medieninhaberin, Verlegerin und Herausgeberin:
Bundesministerium für Bildung, Wissenschaft und Forschung
Gruppe IT und Medien
Minoritenplatz 5, 1010 Wien
Tel.: +43 1 531 20-0
www.bmb.gv.at
Inhalt: BKA, GovCERT und BMBWF
Grafische Gestaltung: BKA Design & Grafik
Cover: thinkstock.com/macbrianmun
Druck: BMBWF
Wien, 2018

Sind Sie sicher?

Informationssicherheit in der
öffentlichen Verwaltung

Verantwortung trifft uns »alle«

Die verschiedenen Sicherheitsvorfälle der Vergangenheit zeigen anschaulich, wie rasch sensible Daten der öffentlichen Verwaltung in falsche Hände geraten können.

Oft sind es nur Kleinigkeiten, die man zu beachten hat, um eine unerwünschte Offenlegung von Daten zu vermeiden oder um Zugänge zu Systemen besser abzusichern.

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.

Einige Grundregeln im alltäglichen Verhalten am Arbeitsplatz

- Wenn Sie den PC-Arbeitsplatz verlassen, aktivieren Sie die Bildschirmsperre.
- Lassen Sie wichtige Unterlagen weder am Schreibtisch noch elektronisch am PC oder nach Besprechungen offen liegen, sondern versperren Sie diese (Schreibtischlade oder PC-Sperre) bzw. nehmen Sie sie mit in Ihr Büro.
- Wenn Sie unterwegs sind, achten Sie darauf, dass vertrauliche Informationen nicht auf Ihrem Notebook oder Smartphone ungeschützt verfügbar sind.
- Verwenden Sie unterschiedliche Passwörter für die verschiedenen Benutzerkonten und Anwendungen. In vielen Fällen wird statt eines Benutzernamens die E-Mail-Adresse verwendet, weshalb Angreifer dann automatisch Zugriff auf weitere Accounts hätten.

- 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 bzw. Dokumente mit personenbezogenen Informationen (zB Schülerdaten, Konferenzprotokolle, Prüfungslisten u.a.) niemals über das offene Internet ohne zusätzlichen Schutz. Verwenden Sie sichere Anwendungen wie etwa das Elektronische Aktensystem oder die zur Verfügung gestellten (Schul-)Verwaltungsprogramme für diese Aufgaben.
- Wenn Sie Verdacht auf ein Sicherheitsproblem oder einen Sicherheitsvorfall 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.

Einige Grundregeln für sichere Zugangsinformationen und Passwörter

Passwörter und Pin-Codes sind der Schlüssel zu unseren Informationssystemen und stellen damit einen besonderen Wert dar. Besondere Sicherheit bieten Zugangsmechanismen mit zwei Komponenten, nämlich Wissen (Passwort) und Besitz (Karte oder Handy), wie es z. B. die Bürgerkarte oder die Handysignatur umsetzen.

Zusätzlich zur Eingabe eines Passwortes kommt eine weitere Sicherheitskomponente z. B. in Form eines auf eine hinterlegte Handynummer als SMS übermittelten und nur für einen sehr eingeschränkten Zeitraum von wenigen Minuten gültigen Pin-Codes zum Tragen. Selbst wenn Passwörter in die falschen Hände gelangen, erhalten

Unbefugte auf diese Weise keinen Zugriff auf das Benutzerkonto. Nachfolgend einige Maßnahmen für sichere Passwörter:

- Passwörter sind in regelmäßigen Abständen zu ändern.
- Passwörter dürfen auf keinen Fall weitergegeben werden. Bei vom Dienstgeber bereitgestellten Systemen kann dies als Dienstpflichtverletzung ausgelegt werden.
- Geben Sie Passwörter immer unbeobachtet von Dritten ein.
- Wenn Sie den Verdacht haben, dass Ihr Passwort einem Dritten bekannt ist, ändern Sie es umgehend.
- Schreiben Sie Passwörter nirgends auf. Wenn nicht anders möglich, versperren Sie diese eventuell in einem elektronischen Passwort-Safe.
- Verwenden Sie nicht das gleiche Passwort im dienstlichen Bereich wie auch im privaten Bereich (z. B. bei sozialen Netzen usw.) bzw. verwenden Sie grundsätzlich immer unterschiedliche Passwörter für die verschiedenen Benutzerkonten und Anwendungen.
- Es gilt das Grundprinzip: Das Passwort muss für Sie leicht merkbar, aber für andere schwer erratbar bzw. aufgrund seiner Merkmale nicht ableitbar sein (wie dies z. B. bei einem Geburtsdatum der Fall wäre).
- Verwenden Sie bei der Gestaltung des Passwortes immer eine Kombination aus Buchstaben, Ziffern und Sonderzeichen. Helfen Sie sich mit Eselsbrücken, z. B. den Anfangsbuchstaben eines für Sie gut merkbaren Satzes mit Ziffern und Sonderzeichen.

Einige Grundregeln für Sicherheit auch außerhalb des Büros

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

- Nehmen Sie nur jene Daten mit, die Sie auch tatsächlich benötigen.
- Achten Sie bei der Verwendung des Notebooks, Tablets, Smartphones u. a. in öffentlichen Bereichen (Flughafen, Bahnhof usw.) darauf, dass niemand Ihre vertraulichen Informationen mitliest.
- Auf Dienstreisen mittels Flug oder Bahn behalten Sie alle Ihre elektronischen Geräte und Speichermedien (Datenstick u. a.) immer bei sich im Handgepäck. Lassen Sie Notebook, Tablet, Smartphone, Datenstick usw. nicht sichtbar z. B. im Auto oder in anderen Bereichen liegen.
- Beachten Sie, dass vertrauliche Informationen, auch wenn sie am Notebook abgespeichert sind, in einem sicheren Bereich bzw. verschlüsselt abgelegt werden.
- Achten Sie bei Ihrem Notebook, Smartphone usw. auf einen stets aktuellen Virenscanner.
- Wenn Sie sich in ein öffentliches WLAN (»Hotspot«) einwählen, surfen Sie am besten über ein Betriebssystem-Nutzerkonto mit eingeschränkten Zugriffsrechten und geben Daten ausschließlich über SSL-verschlüsselte Websites ein (erkennbar an »https://« und einem Schloss-Symbol entweder neben der Adressleiste oder am unteren Bildschirmrand). Viele öffentliche Verbindungen sind nicht ausreichend geschützt.

Einige Grundregeln für eine 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.

- 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 nach Möglichkeit 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 (siehe Hinweise SSL-Verschlüsselung).
- Achten Sie beim Herunterladen besonders auf Dateien, die für Sie unbekannte Endungen (also nicht .doc, .xls, .pdf usw.) aufweisen.
- Antworten Sie niemals auf Spam-E-Mails, weder um Fragen zu beantworten, noch um mitzuteilen, dass Sie diese lästigen Zusendungen nicht mehr wollen. Damit bestätigen Sie nur, dass

es sich um eine gültige E-Mail-Adresse handelt und bekommen umso mehr Spam.
- Überlegen Sie genau, welche Daten Sie im Internet von sich preisgeben. Im Netz ist es oft schwierig, seine Rechte bei Datenmissbrauch durchzusetzen.

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.
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 die IT-Abteilung im BMB unter zentraleinformatik@bmb.gv.at zur Verfügung.

Notizen