INFOSIC

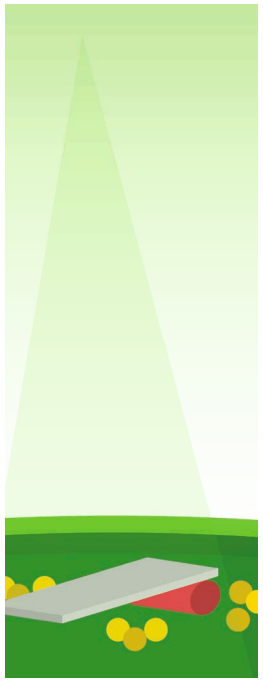
als E-Learning-Angebot

Beta-Tester gesucht!

Künftig möchten wir Sie gerne beständig und aktuell zur Thematik fortbilden – mithilfe eines E-Learning-Angebots zur Informationssicherheit am Arbeitsplatz. In zehn Kapiteln werden Sie eine Menge erfahren, bspw. über Virenschutz und Social Media, über mobile Endgeräte, Passworte und Phishing-Mails. Darüber hinaus werden Sie lernen, in welchem Umfang Daten im Sächsischen Verwaltungsnetz und auf Ihrem PC automatisch geschützt werden, und welchen Beitrag Sie persönlich zum Schutz von Daten und Informationen aus Ihrem Arbeitsbereich leisten können.

Das zukünftige E-Learning-Angebot zur Informationssicherheit am Arbeitsplatz befindet sich derzeit in einer Testversion.
Wenn Sie Interesse haben ausgewählte Kapitel im Januar 2017 über einen Zeitraum von drei Wochen zu studieren, melden Sie sich bitte unter Angabe Ihres Namens und Ihrer Behörde bei infosic@smi.sachsen.de unter dem Betreff: „Testperson".

Sie erhalten noch im Dezember eine Einladung zu einer einstündigen Eröffnungsveranstaltung voraussichtlich in der zweiten Januarwoche. Im Anschluss an Ihr Selbststudium bekommen Sie von uns einen Einschätzungsbogen, dessen Beantwortung uns sehr weiter helfen wird, das E-Learning-Angebot zielgruppengerecht weiter zu entwickeln.

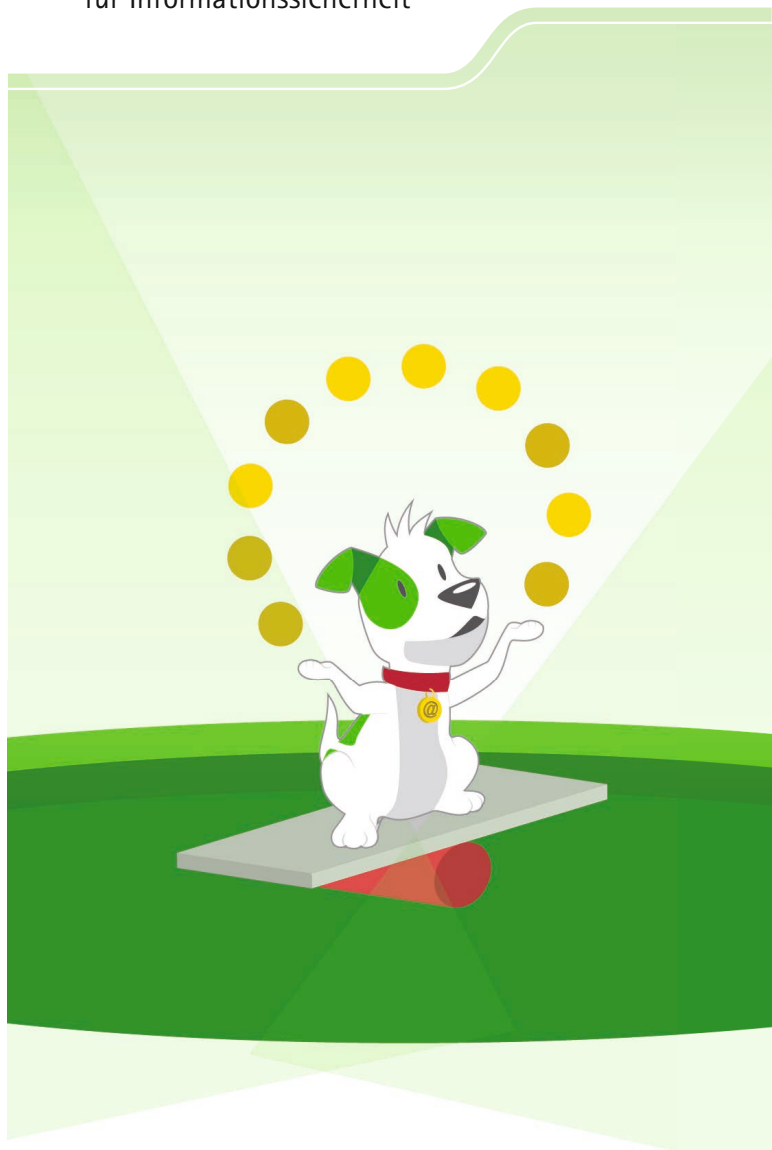


Herausgeber:
Sächsisches Staatsministerium des Innern
Wilhelm-Buck-Straße 2
01097 Dresden
Redaktion:
Referat 65 Informationssicherheit in der Landesverwaltung, Cybersicherheit
Gestaltung und Satz:
Torux - Kreativleistung nach Maß, Dresden
Druck:
Flyeralarm
Redaktionsschluss:
Oktober 2016
Motive:
Torux, Dresden 2016

STAATSMINISTERIUM DES INNERN | Freistaat SACHSEN

10 Goldene Regeln

für Informationssicherheit



10 Goldene Regeln

für Informationssicherheit

1. Software auf dem aktuellen Stand halten

Bei Betriebssystemen und Anwendungen werden immer wieder Schwachstellen bekannt, die die Sicherheit Ihres Computers gefährden. Installieren Sie regelmäßig die Aktualisierungen der Hersteller. Gut für Sie: In Ihrer Behörde erledigt das bereits Ihr IT-Service.

2. Aktuellen Virenscanner verwenden

Ein aktueller Virenscanner gehört zum Basisschutz eines jeden Computers. Achten Sie darauf, dass dieser aktiviert ist und auf dem aktuellen Stand gehalten wird. Der Virenscanner sollte jedoch nicht zur Gedankenlosigkeit verleiten, da er keinen absoluten Schutz bieten kann! Gut für Sie: In den zentralen Diensten des SVN, in den Behörden und auf Ihrem Arbeitsplatz-PC gibt es einen dreistufigen Virenschutz.

3. Daten mit einer Firewall schützen

Eine Firewall schützt Ihren Computer vor unberechtigten Zugriffen aus dem Internet bzw. aus dem Netzwerk, in dem Sie arbeiten. Die oft bereits im Betriebssystem enthaltene Firewall sollte deshalb unbedingt dauerhaft aktiviert werden. Gut für Sie: Auf Ihrem Arbeitsplatz-PC gehen Sie automatisch mit Firewall ins Netz.

4. Sichere Passworte verwenden

Gute Passwörter sind mindestens 8, besser 10 Zeichen lange Kombinationen von Anfangsbuchstaben individueller Merksätze oder eine Aneinanderreihung von 3-4 beliebigen Wörtern, ideal mit Ziffern und Sonderzeichen versetzt. Wichtig: Passwörter für dienstliche, private und finanzielle Angelegenheiten müssen strikt getrennt werden und dürfen nie weitergegeben werden!

5. Nicht mit Administratorrechten arbeiten

Wenn Sie mit Administratorrechten auf Ihrem Computer arbeiten, haben auch Schadprogramme uneingeschränkten Zugriff auf Ihr System und können so ihre volle Wirkung entfalten. Arbeiten Sie im Alltag deshalb unter einem Benutzer-Konto mit eingeschränkten Rechten. Gut für Sie: Auf Ihrem Arbeitsplatzrechner sind die Zugriffsrechte automatisch eingeschränkt.

6. Vorsicht bei E-Mail-Anhängen und Links

Um den Eintritt schädlicher Software zu vermeiden, sollten Sie nie leichtfertig Anhänge und Links in E-Mails von Absendern öffnen, von welchen Sie keine Mail erwarten. Oft sind bösartige E-Mails auch an Rechtschreibfehlern oder am fehlenden dienstlichen Kontext erkennbar. Jeder geöffnete Anhang oder geklickte Link aus einer E-Mail heraus kann die Sicherheit Ihres Computers und des gesamten Netzes gefährden. Im Zweifel oder bei einem ungewöhnlichen Verhalten des Computers nach der Öffnung verdächtiger E-Mails sollten Sie stets Ihren IT-Service kontaktieren.

7. Daten regelmäßig sichern

Eine regelmäßige Sicherung mittels „Backup" Ihrer wichtigen Daten schützt diese vor Verlust. Nur gesichert ist sicher! Gut für Sie: In Ihrer Behörde erstellt Ihr IT-Service regelmäßige Backups.

8. Informationssicherheit betrifft nicht nur den Computer

Wenn Sie Ihr Büro verlassen - und sei es nur für eine kurze Kaffeepause - sichern Sie Ihr Büro vor unbefugtem Zugriff, indem Sie die Tür verschließen. Sensible Informationen sind auch auf Papier ein lohnenswertes Objekt für Datendiebe.

9. Nie aus Drucksituationen heraus handeln

Werden Sie hellhörig, wenn Sie um die Herausgabe von persönlichen Informationen von Ihnen oder von Dritten gebeten werden – egal ob Passwort, Telefonnummer oder Informationen aus dem Terminkalender. Gleiches gilt, wenn unerwartet per E-Mail oder Telefon von angeblich „höchster Stelle" geheim zu haltende Handlungen angeordnet werden. Handeln Sie nie aus einer Drucksituation heraus! Atmen Sie durch und gehen Sie der Sache mit einem Kollegen auf den Grund.

10. Informationen nicht leichtfertig preisgeben

Vom zu lauten Gespräch über Dienstliches in der Straßenbahn bis hin zu Einträgen in sozialen Netzwerken mit vertraulichen Informationen Ihrer Behörde oder Hinweisen zu Ihrem Passwort: Tragen Sie Sorge dafür, dass Dienstliches auch dienstlich bleibt.