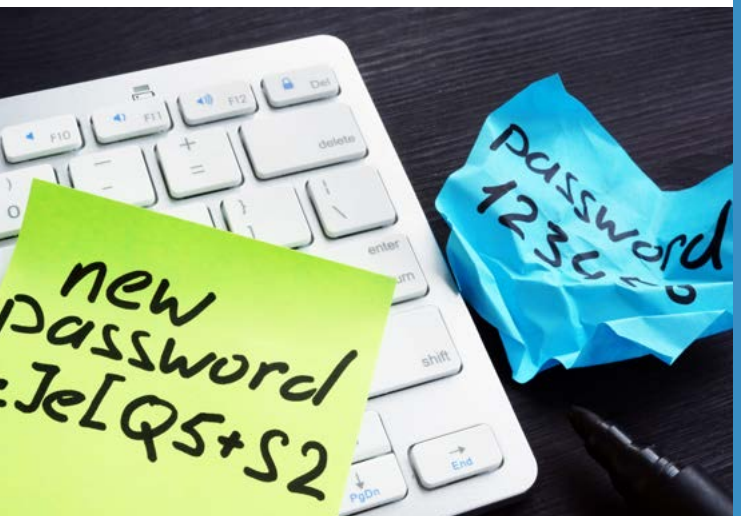
In Homeoffice-Zeiten ist der sichere Umgang mit Passwörtern noch wichtiger geworden. Deshalb hat die Landesverwaltung die Regeln neu festgelegt.

Beim Umgang mit Daten auf Rechnern und im Behördennetzwerk muss die Landesverwaltung sicherstellen, dass nur berechtigte Bedienstete zugreifen und das auch nur im unbedingt notwendigen Umfang tun können. Deshalb muss sich jeder Bedienstete mit einem Passwort authentifizieren und seine Zugangsberechtigung nachweisen.

Die Bezeichnung „Passwort“ darf man nicht wörtlich nehmen: Heute muss man „Passphrasen“ denken, also längere, möglichst komplizierte Zugangscodes, die den Entschlüsselungsprogrammen das Leben so schwer wie möglich machen.

Die Verwendung geeigneter Passwörter ist von besonderer Bedeutung, seitdem dienstliche Daten häufiger im Homeoffice ohne den Schutz des Gebäudes der Behörde verarbeitet werden. Weil Rechenleistung immer besser wird, können Passwörter schneller geknackt werden. Aus diesem Grund wurde für die Thüringer Landesverwaltung eine neue Passwortrichtlinie erlassen. Die jeweils aktuelle Passwortrichtlinie finden Sie im Intranet der Landesverwaltung (▸ http://intranet.thlv.de) unter „Informationssicherheit“.



www.thueringen.de

digitale Services
verwaltung.thueringen.de

Herausgeber:
Thüringer Finanzministerium
Informationssicherheitsbeauftragter des Freistaats
Ludwig-Erhard-Ring 7
99099 Erfurt

Bilder:
Rogge GmbH, Bildmontagen unter Verwendung von Motiven aus AdobeStock, ©chinnarach (Titel), ©peshkova (innen oben), © thodonal (innen unten), ©Vitalii Vodolazskyi (S. 5)
Text und Layout:
Rogge GmbH, Weimar

Freistaat Thüringen

Sicheres Passwort-management

Was Bedienstete tun und vermeiden sollten, um ihre Zugangscodes zu schützen

Informationssicherheit

Achten Sie für ein sicheres Passwortmanagement auf diese Hinweise:

Länge ist besser

Alle Passwörter müssen aus mindestens 12 Zeichen bestehen, Administrator-Passwörter aus 16 Zeichen. Verwenden Sie einen Mix aus den Elementen: Zahlen, kleinbuchstaben, GROSSBUCHSTABEN, Sonderzeichen.

Keine leicht zu erratenden Passwörter verwenden

Leicht zu erratende Passwörter sind zum Beispiel solche mit:

- häufigen Zeichenwiederholungen („AAAAA“ oder „BBB666“),
- Buchstabenkombinationen, die im Nutzernamen vorkommen,
- Informationen aus dem Lebensbereich des Benutzers,
- Zeichenkombinationen, die den vorherigen Passwörtern ähneln und
- Zeichenkombinationen, die Suchbegriffen in Wörterbüchern und Lexika entsprechen.

Moeglichst keine ä, ö und ü verwenden

Umlaute könnten die Eingabe des Passwortes aufgrund unterschiedlicher Tastaturbelegung unnötig erschweren.

Eigener Code für jede Anwendung

Nutzen Sie nie dasselbe Passwort für mehrere Zugänge.

Sichere Aufbewahrung

Schließen Sie niedergeschriebene Passwörter ein.

Regelmäßiger Wechsel

Je länger man ein Passwort benutzt, umso größer ist die statistische Wahrscheinlichkeit, dass es geknackt werden oder in falsche Hände gelangen kann. Alle Passwörter sollten deshalb regelmäßig einmal im Jahr gewechselt werden.

Passwörter nicht weitergeben

Unter keinen Umständen dürfen Dritte mit Ihren Zugangsdaten agieren.

Übersicht bewahren

Verwenden Sie einen elektronischen Passwort-Safe, wenn Sie befürchten, wegen der vielen Zugangscodes die Übersicht zu verlieren. Ihr IT-Bereich hält hierfür eine Empfehlung bereit.

Kompromittierte Passwörter ändern

Wenn Sie die Befürchtung haben, dass Dritte Zugang zu Passwörtern erlangt haben, müssen Sie diese unverzüglich ändern und den Vorfall dem Vorgesetzten und dem zuständigen Administrator/IT-Sicherheitsbeauftragten melden.

Kampagne SECURITY AWARENESS
Eine Handreichung des
Thüringer Finanzministeriums
für die Arbeit mit digitalen Medien

Ansprechpartner/
IT-Sicherheitsbeauftragte(r):

Name:

Dienststelle:

Telefon:

E-Mail: