Amtssigniert. SID2015061014193
Informationen unter: amtssignatur.tirol.gv.at

Amt der Tiroler Landesregierung

Verwaltungsentwicklung

Mag. Mathias Winkler

Telefon +43 512 508 1942
Fax +43 512 508 741945
verwaltungsentwicklung@tirol.gv.at

DVR:0059463

An alle Nutzerinnen und Nutzer des Portal Tirol

Zwingender Passwortwechsel

Geschäftszahl VEntw-IT-510/84-2015
Innsbruck, 03.06.2015

Sehr geehrte Damen und Herren,

Sie wurden aufgefordert, ihr Passwort am Portal Tirol zu ändern. Diese Passwortänderungsaktion ist vom Land Tirol beauftragt, wir bitten dafür um ihr Verständnis. Durch einen Passwortwechsel können die Passwörter an aktuelle Anforderungen angepasst werden und eventuell gestohlene / weitergegebene Passwörter werden ungültig.

Ihr Passwort ermöglicht in Kombination mit ihrer Benutzerkennung den Zugang zu verschiedenen IT-Services des Landes und des Bundes über das Portal Tirol. Im Portal Tirol dürfen Zugangsdaten nicht weitergegeben werden, da jede Handlung in einer Portalanwendung der angemeldeten Person zugeordnet wird. Sollten ihre Zugangsdaten anderen Personen bekannt sein, kann ein „Unschuldsbeweis“ für bspw. illegale Datenabfragen möglicherweise nicht erbracht werden. Klarerweise ist deshalb geboten, dass alle Zugangsdaten mit größtmöglicher Sorgfalt und dem Stand der Technik entsprechend geschützt werden.

Beim sicheren Umgang mit Passwörtern haben sich in den letzten Jahren entscheidende Rahmenbedingungen geändert:

1.) **Einfache Passwörter können heute sehr einfach geknackt werden**:
   a. Für Attacken gibt es eigene „Wörterbücher“ (Listen häufiger / bekannter Passwörter, aller bekannten Wörtern, Namen,…) Diese Wörterbücher sind für alle Sprachen und übliche Abwandlungen (Margarete - Gretchen) bzw. Verfälschungen einzelner Buchstaben

(w!k!p3d!4 – wikipedia) verfügbar. Auch das Ein- oder Anfügen von Jahreszahlen oder Kombinationen aller Wörter werden eingesetzt.

b. Die Rechenleistung hat massiv zugenommen, mit jedem Smartphone und dem richtigen Programm kann heute ein 7-stelliges Passwort durch ausprobieren aller Kombinationen in wenigen Stunden geknackt werden.

c. Passwörter sind deshalb umso sicherer, je länger diese sind und aus je mehr Zeichengruppen diese bestehen: Groß/Kleinbuchstaben, Zahlen, Sonderzeichen. Derzeit gelten noch 8-stellige Passwörter mit Zeichen aus 3 Gruppen als ausreichend sicher, in absehbarer Zeit wird ein neuntes Zeichen erforderlich werden.

2.) **Jeder Benutzer hat eine Vielzahl von Zugängen, Standardpasswörter sind ein hohes Risiko:**
Heute gibt es sehr viele Online-Services (Shops, Webmail, Online-Banking, Cloud, Social Media,…), die jeweils mit Benutzername und Kennwort abgesichert sind. Viele aktive Internetnutzer nutzen eine Vielzahl solcher Dienste. Als „Benutzername" zur Anmeldung fungiert dabei oft eine E-Mailadresse, die Kennwörter müssen selbst gewählt werden. Um den Überblick zu wahren, verwenden viele Personen dieselbe E-Mailadresse und dasselbe Passwort. Nicht alle Online-Dienste schützen ihre Systeme aber ausreichend. In den letzten Jahren wurden einige dieser Dienste (auch namhafter Unternehmen wie Sony oder Adobe) gehackt und Zugangsdaten inkl. Passwörter gestohlen, teilweise auch veröffentlicht.

Hacker versuchen mit diesen gestohlenen Zugangsdaten ihr Glück bei weiteren Diensten (siehe auch „Wörterbücher"). Eine Mehrfachverwendung eines Passwortes für verschiedene Dienste ist deshalb keinesfalls empfehlenswert.

3.) **Passwörter dürfen in keinem Fall weitergegeben werden:**
Gerade im Berufsleben wurden früher die Passwörter der Kolleginnen und Kollegen oft ausgetauscht oder auf gemeinsame Listen geschrieben um im Urlaubs/Krankheitsfall auf notwendige dienstliche Daten zugreifen zu können. Aktuelle Programme unterstützen Benutzerrollen mit Vertretungsfunktionen. Sollten solche Funktionalitäten nicht aktiviert sein, können im Notfall Administratoren jederzeit neue Passwörter setzen und damit ggf. dem Dienstgeber Zugriff auf wichtige Informationen geben (unter Einhaltung von arbeitsrechtlichen Einschränkungen).

Sobald sie ihr Passwort weitergeben, haben sie keine Kontrolle mehr darüber, wer sich mit ihren Daten anmeldet und welche Handlungen ihnen zugeordnet werden. Auch wenn sie den Personen trauen, denen sie ihr Passwort geben, können sie sich nie sicher sein, ob diese sorgfältig behandelt werden.

4.) **Passwörter aufschreiben ist (bei korrekter Vorgehensweise) vertretbar:**
Da also jede Person viele, komplexe und nicht zusammenhängende Passwörter haben soll und diese auch öfters gewechselt werden sollen, ist das Aufschreiben von Passwörtern dann vertretbar, wenn dies sicher erfolgt und sie sicher verwahrt werden. Für eine sichere elektronische Verwahrung gibt es eigene Programme die wiederum mit einem sogenannten Masterpasswort abgesichert sind (zB KeePass), Passwörter auf Papier sollten z.B. in der Geldtasche (ohne Hinweis auf den zugehörigen Service und Benutzernamen) aufbewahrt werden. Keinesfalls dürfen Passwörter an Pinnwänden, mit Post-ITs am Arbeitsplatz oder unter der Tastatur aufbewahrt werden.

Weitere Hinweise zum Thema Passwortsicherheit finden sie zB hier:

https://www.onlinesicherheit.gv.at/mitarbeiterinnen/passwort-sicherheit/70963.html

http://www.heise.de/security/artikel/Sinnvolle-Ergaenzungen-zum-Virenscanner-1106122.html?artikelseite=3

Sollten Sie Fragen haben und ihnen die Hilfeseite unter Portal Tirol Wiki - Mein Passwort keine Antworten geben, wenden Sie sich bitte an die TGN-Hotline bei der DVT bzw. an servicedesk@cnt.at.

Für allgemeine Fragen steht Ihnen das Sachgebiet Verwaltungsentwicklung unter verwaltungsentwicklung@tirol.gv.at jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen

Mathias Winkler – IT-Koordinator