Schnellzugang

An Windows 10 mit PIN statt Kennwort anmelden

Es ist vertrackt: Je mehr Zeichen ein Kennwort enthält, umso schwerer lässt es sich knacken, doch umso nerviger ist es auch, es nach jeder Bildschirmsperre erneut einzutippen. Unter Windows 10 hilft das Verwenden einer zusätzlichen PIN aus dem Dilemma.

Von Axel Vahldiek

Egal, ob Microsoft-Konto oder herkömmliches lokales Benutzerkonto: Für beide Arten können Sie unter Windows 10 zum lokalen Anmelden an das System eine PIN statt eines Kennworts verwenden. Sie brauchen also nur ein paar selbst gewählte Ziffern einzutippen und schon sind Sie drin. Das Kennwort ist nur noch selten erforderlich, etwa bei Zugriffen übers Netzwerk oder wenn Sie Ihre PIN vergessen haben. Wenn das Upgrade auf Windows 10 Version 1703 installiert ist (Creators Update), spielt bei der Eingabe der PIN via Ziffernblock nicht mal mehr der Status der Numlock-Taste eine Rolle. Geeignet ist der Einsatz der Ziffernfolge überall dort, wo Ihnen beim Eintippen niemand über die Schulter schauen kann.

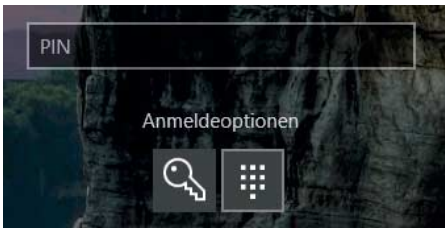
Sicher?

Ob der Einsatz einer PIN sicher ist, hängt vor allem davon ab, welche Ziffernkombination Sie wählen. Klassiker wie 0000 oder 1234 verbieten sich von selbst, aber auch andere aufeinanderfolgende Zahlen sowie Geburtsjahre sollten Sie meiden. Verwenden Sie eine möglichst zufällige Zahl. Die PIN wird noch sicherer, je mehr Ziffern sie enthält, doch je länger sie ist, umso näher sind Sie auch wieder am Ausgangsproblem der Mühsal des Eintippens. Ein simpler Weg zum Verlängern: Geben Sie die einzelnen Ziffern oder die gesamte PIN jeweils zweimal hintereinander ein. So brauchen Sie sich nur vier Ziffern zu merken, um eine achtstellige PIN nutzen zu können.

Ein simples Durchprobieren aller denkbaren Kombinationen verhindert Windows. Ein Angreifer hat vier Versuche, dann muss er eine angezeigte Passphrase abtippen. Nach dem fünften Versuch ist ein Neustart fällig. Versucht der Angreifer es danach weiter, muss er nach weiteren vier Versuchen 30 Sekunden warten, bevor nach erneuter Passphrasen-Eingabe und dem fünften Versuch wieder ein Neustart fällig wird. Setzt er das Spiel fort, verlängert Windows die Wartezeit immer weiter, erst auf 1 Minute, dann auf 2, 5, 10 und 30 Minuten, danach gehts bereits um Stunden. Die Wartezeit wird also immer mindestens verdoppelt und überschreitet schnell die Dauer eines Menschenlebens. Sofern ein Angreifer also nicht gleich am Anfang einen Zufallstreffer landet, wird er Ihre PIN nicht knacken können.

Einrichten

Den Dialog zum Einrichten einer PIN finden Sie in den Einstellungen unter „Konto/Anmeldeoptionen“. Der Dialog fordert zuerst die Eingabe Ihres Kennworts, anschließend können Sie eine beliebige Zahlenfolge eingeben, die Sie wiederholen müssen. Die minimale Länge beträgt 4, die maximale 127 Ziffern. Erlaubt sind wirklich nur Ziffern, also weder Buchstaben oder Sonderzeichen. Die PIN gilt ab sofort, ein Neustart ist nicht nötig. Beim Anmelden können Sie sich den bislang obligatorischen Druck auf die abschließende Enter-Taste übrigens sparen, Sie sind schon nach Eintippen der letzten Ziffer „drin“.



Bei Bedarf können Sie sich jederzeit statt mit PIN wieder mit Ihrem Kennwort anmelden. Dazu einfach unterhalb des PIN-Eingabefeldes erst auf den Link „Anmeldeoptionen“ und dann auf den Schlüssel klicken.

Die PIN gilt nur für diese Windows-Installation, selbst wenn Sie deren Einstellungen per Microsoft-Konto auf andere Installationen synchronisieren.

Das Kennwort brauchen Sie wie erwähnt trotzdem noch. Es kann nun aber deutlich länger und damit sicherer ausfallen, weil Sie es ja nicht mehr ständig eintippen müssen. Sollten Sie also bislang aus Bequemlichkeit ein pragmatisch kurzes Kennwort verwendet haben, ist nun ein guter Zeitpunkt, es in ein sicheres langes zu ändern. Der Dialog dafür ist auf der gleichen Seite der Einstellungen. Doch Obacht: Wenn Sie es nicht mehr täglich mehrfach eintippen, könnte es irgendwann in Vergessenheit geraten. Schreiben Sie es also besser auf einen Zettel und verwahren Sie diesen an sicherer Stelle, am besten in einem Tresor.

PIN-Komplexität

Unter Windows 10 Pro und Enterprise lassen sich einige Einstellungen für die PIN-Eingabe mit Gruppenrichtlinien steuern. Sie finden sie im Gruppenrichtlinien-Editor gpedit.msc unter „Computerkonfiguration/Administrative Vorlagen/System/PIN-Komplexität“. Dort können Sie beispielsweise die minimale und maximale Länge der PIN beeinflussen, zusätzlich zu Ziffern auch Groß-, Kleinbuchstaben oder Sonderzeichen erzwingen sowie Ablauf-Daten festlegen.

Für den heimischen Einsatz dürfte das aber alles unnötig sein und auch im Unternehmen sollten Sie nur mit Bedacht eine erhöhte Komplexität erzwingen. Denn sonst sind Sie schnell wieder beim Ursprungsproblem.

Wenn alle gucken …

Falls Ihnen jemand beim Anmelden an Windows zuguckt, gilt das Gleiche wie am Geldautomaten: Schirmen Sie die Eingabe mit der anderen Hand ab. Alternativ können Sie, statt die PIN einzugeben, darunter auf „Anmeldeoptionen“ klicken. Dort finden Sie in der Standardeinstellung zwei Symbole, das rechte führt Sie zur altbekannten Kennwort-Eingabe. Sie haben also stets die Wahl, ob Sie in diesem Moment die kurze PIN oder das lange Kennwort nutzen wollen. Tipp: Verwenden Sie für das Kennwort abwechselnd Zeichen rechts und links auf der Tastatur, das erschwert fremden Augen das Mitlesen. Üben Sie zudem das Eintippen, bis es so schnell geht, dass fremde Augen nicht mehr folgen können. *(axv@ct.de)* c't