Beispiel:

Angenommen der Startpunkt ist B2, die Richtung rechts unten (im 45-Grad-Winkel) und die Länge 10 Zeichen. Hieraus ergibt sich folgendes Passwort: a T t c ; Q d r Ä L

Der wesentliche **Vorteil** dieses Verfahrens ist, dass man ohne Kenntnis von Startpunkt und Richtung das Passwort nicht ermitteln kann. Hierdurch lassen sich recht komplexe Passwörter verhältnismäßig leicht erstellen, ohne dass die Gefahr des Vergessens oder des Aufschreibens besteht. Auch wenn die Möglichkeit, das Passwort festzustellen, sehr gering ist, sollte die Karte nicht öffentlich ausgelegt werden. Als **Nachteil** ist anzuführen, dass bei einem Verlust der Karte eine Authentisierung, da das Passwort unbekannt ist, nicht mehr möglich ist. Aus diesem Grund sollten mindestens zwei Kopien der Passwortkarte getrennt voneinander sicher aufbewahrt werden.

M/5.2.3 2-Faktor-Authentisierung

Aus dem Vorstehenden ist deutlich geworden, dass eine Authentisierung, die allein auf dem Faktor Wissen (Passwort) basiert, nur begrenzt sicher ist. Insbesondere personenbezogene oder anderweitig unternehmenskritische Daten sollten durch Hinzunahme mindestens eines weiteren Faktors zur Authentisierung weiter geschützt werden (2-Faktor-Authentisierung). Bei der 2-Faktor-Authentisierung werden zwei verschiedene Authentisierungsmethoden (Wissen, Besitz und Biometrie) kombiniert und die Sicherheit erhöht. Passwort und PIN ist keine 2-Faktor-Authentisierung, da hier zwei Authentisierungsmethoden derselben Kategorie verknüpft werden.

Ein gutes Beispiel für eine 2-Faktor-Authentisierung ist der Geldautomat. Hier wird „Wissen“ mit „Besitz“ kombiniert. Um Geld abheben zu können, ist sowohl der Besitz der entsprechenden Geldkarte (Faktor „Besitz“) als auch die Kenntnis einer persönlichen PIN (Faktor „Wissen“) notwendig.

One-Time-Password-Token (OTP-Token nicht zu verwechseln mit dem One-Time-Pad – vgl. M/1.4) sind Einmalpasswörter, die nach unterschiedlichen Algorithmen berechnet und durch Hardware- oder Software-Token erzeugt werden. Wie sich aus dem Begriff ableiten lässt, sind derartig erzeugte Passwörter nur einmalig einsetzbar. Danach verlieren sie ihre Gültigkeit (z. B.

TAN). Bei Hardware-Token handelt es sich um portable Geräte in der Größe eines USB-Sticks.

Ein Hardware-Token für ein One-Time-Password generiert einen Zahlencode, der vom Authentisierungs-Server validiert wird. Bei Hardware-OTP-Token gibt es drei Varianten.

Variante 1 (Ereignisbasiertes OTP)

Hier wird das OTP per Knopfdruck auf einem Hardware-Token erzeugt (z. B. mTAN-Verfahren beim Onlinebanking).

Variante 2 (Zeitbasiertes OTP)

Bei diesem wird das OTP für eine bestimmte Gültigkeitszeit auf dem Gerätedisplay angezeigt (z. B. SecurID der RSA Security Inc.).

Variante 3 (Challenge Response)

Hierbei wird durch einen Server eine Aufgabe, die sogenannte Challenge, vorgegeben. Diese Aufgabe muss der anfragende Client beantworten (sogenannte Response). Der Client erhält einen Wert des Servers als Eingabe und berechnet darauf basierend ein Einmalkennwort.

Die dargestellten Varianten gibt es als Hard- und Software-Implementierungen. Der wesentliche Nachteil von Software-Implementierungen ist deren Anfälligkeit für Manipulationen, beispielsweise durch Computerviren. Ein Beispiel für ein Software-Token ist das RSA SecurID Toolbar Token, das vom Microsoft Internet Explorer und Mozilla Firefox unterstützt wird.

Eine weitere Möglichkeit der 2-Faktor-Authentisierung bietet der Einsatz von **Biometrie**, der jedoch umstritten ist, da es sich um eindeutige persönliche Merkmale handelt. Kann oder soll trotzdem nicht auf den Einsatz von Biometrie verzichtet werden, sollte immer hinterfragt werden, auf welche Weise welche Daten gescannt und gespeichert werden, ob der Datentransfer verschlüsselt und die Speicherung besonders geschützt sind bzw. ob die persönlichen Merkmale aus der Datenspeicherung rekonstruiert und missbraucht werden könnten. Aufgrund der hohen Datensensibilität müssen die Daten ferner vor unbefugtem Zugriff besonders geschützt sein (vgl. M/5.1.4).

Beispiel: Fingerprint Swipe Reader an Notebooks

Letztlich kann eine 2-Faktor-Authentisierung auch über **SmartCards** und **digitale Zertifikate** realisiert werden. Bei einem digitalen Zertifikat dient dieses dem Benutzer als Ausweis gegenüber dem System. Beim Anmeldungsprozess am System überprüft der Server dann zusätzlich zu den Login-Daten, ob der Benutzer über ein gültiges digitales Zertifikat verfügt. Häufig werden Zertifikate auf unterschiedlichen Geräten wie SmartCards oder USB-Sticks gespeichert. Wesentlicher Nachteil bei der Anschaffung und Verwendung von Zertifikaten in großen Umgebungen stellen die meist hohen Kosten und die komplexe Umsetzung der Infrastruktur dar.

M/5.2.4 Passwortgeschützter Bildschirmschoner

Ist ein Benutzer an einem Datenverarbeitungssystem angemeldet, sind die meisten Zugangskontrollmaßnahmen durch die bereits erfolgte Eingabe der erforderlichen Passwörter deaktiviert. Verlässt der Benutzer den Arbeitsplatz kurzfristig, ist das System vor Zugriffen ungeschützt.

In der Regel aktiviert sich nach einem bestimmten Zeitraum (in der Regel nach fünf bis zehn Minuten) ein Bildschirmschoner. Allerdings erfordert die Deaktivierung des Bildschirmschoners oft keine Eingabe eines Passwortes oder die Zeitspanne bis zur Aktivierung des passwortgeschützten Bildschirmschoners ist so lang, dass Unbefugte Zugriff nehmen können.

Um der Gefahr von unbefugten Zugriffen bei kurzzeitiger Abwesenheit zu begegnen, sollten folgende Maßnahmen technischer und organisatorischer Art ergriffen werden:

- Bürotüren sind beim Verlassen, auch bei kurzzeitigen Abwesenheiten, zu verschließen.
- Zusätzlich zur automatischen Aktivierung der Sperre nach einer bestimmten Zeit sollten die Mitarbeiter verpflichtet werden, Rechner manuell zu sperren, z. B. bei Windowsbetriebssystemen durch die Tastenkombination Windows-Taste + L.
- Zur Deaktivierung ist die Eingabe eines Passwortes zwingend erforderlich.