Venen lügen nicht

Sicherheit macht mobil – und das vor allem bei der Arbeit. Biometrische Verfahren wie der Handvenen-Scan schützen Daten auf Laptops effizient und ermöglichen damit ein sicheres Arbeiten beim Kunden. **Von Manuel Gremes**

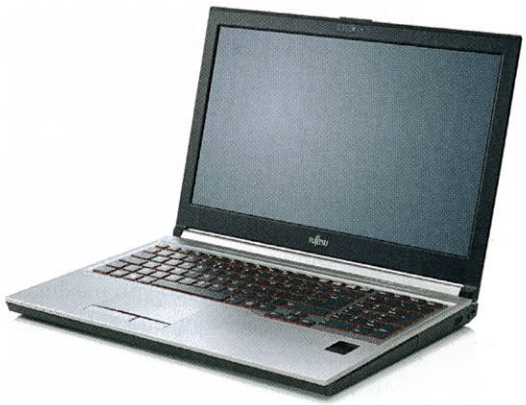

Bild 1: Mobile Workstations müssen nicht nur Leistung, sondern auch ein Plus an Sicherheit bieten. Fujitsu Celsius H730 bietet zum Beispiel ausgefeilte Sicherheitsverfahren wie Handflächenvenen-Scanner. Bild: Fujitsu

Mobile Rechner bieten im Berufsalltag viele Vorteile, zum Beispiel das Arbeiten unmittelbar beim Kunden anstatt am eigenen Schreibtisch. Die neue Flexibilität hat aber auch eine Schattenseite: Zumeist befinden sich zahlreiche sensible und wertvolle Informationen auf Laptop & Co. Ihr Verlust oder Diebstahl kann katastrophale Folgen haben. Schutz vor unbefugtem Zugriff tut also Not. Eine der effektivsten Möglichkeiten zur Absicherung des mobilen Arbeitsplatzes sind biometrische Authentifizierungsverfahren – und insbesondere Handvenen-Scanner. Sie bieten ein Maximum an Sicherheit. Das wird in dem Maß immer wichtiger, in dem leistungsstarke Laptops immer größere Datenmengen aufnehmen und komplexere Aufgaben bewältigen können. Gerade in Bereichen, in denen zum Beispiel aufwändige Entwicklungsunterlagen auf den Rechner geladen werden, dürften auch die Begehrlichkeiten entsprechend hoch sein. Handvenen-Scanner bieten hier die beruhigende Gewissheit, dass niemand außer dem autorisierten Nutzer Zugang zum mobilen Arbeitsplatz hat.

Der Laptop hat sich inzwischen zur nahezu gleichwertigen Alternative zum Desktop gemausert. Mit leistungsstarken Prozessoren, Speicher, Kommunikationstechnologien und Grafikkarten sind die Geräte in der Lage, auch wirklich anspruchsvolle Aufgaben zu bewältigen – etwa in den Bereichen CAD und CAE. Zum Beispiel bieten die Endgeräte der CELSIUS-Reihe von Fujitsu starke Prozessoren der Core-i5- und Core-i7-Range von Intel, ferner Kommunikationstechniken wie WLAN, 3G-/4G-Mobilfunk und Bluetooth sowie USB- und Ethernet-Schnittstellen. Insgesamt bis zu 32 GByte RAM stehen für speicherintensive Anwendungen zur Verfügung; optional können schnelle Solid State Drives (SSDs) oder Solid State Hybrid Drives (SSHDs) genutzt werden. Nicht zuletzt finden Grafikkarten wie die Quadro K von Nvidia mit bis zu 2 GByte GDDR5-VRAM bei den Celsius-Systemen Verwendung.

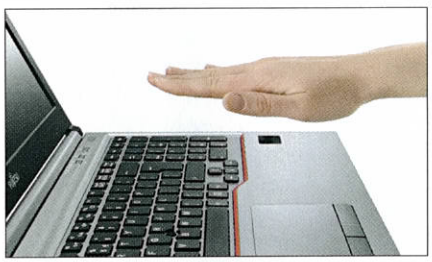

Bild 2: Die biometrische Authentifizierungstechnologie PalmSecure von Fujitsu scannt die Venen der Handfläche. Das Erkennen der Venen erfolgt mithilfe von Infrarot-Licht, ohne dass das Gerät berührt werden muss. Bild: Fujitsu

Passwortschutz nicht ausreichend

Was mobile Geräte mit aktueller Ausstattung so wertvoll macht, sorgt andererseits für eine besondere Anfälligkeit für unbefugte Zugriffsversuche: Wo viel ist, ist auch viel zu holen. Daher ist die Sicherheitsfrage nicht weniger entscheidend für die Praxisfähigkeit als die Leistung und die Kapazität. Zahlen und Daten zu aktuellen Produkten und Projekten, Kundeninformationen und Finanzkennziffern wollen gut geschützt sein, denn sie sind heiß begehrt – vor allem bei der Konkurrenz. Geraten sie in falsche Hände, hat das für das Unternehmen und den betroffenen Mitarbeiter gleichermaßen sehr unerfreuliche Konsequenzen. Wenn es sich nicht gerade um ein zentral implementiertes Passwort-Management handelt, reicht ein einfacher Passwortschutz gegen Datendiebe und -spione nicht aus. Gebraucht wird eine weitaus smartere und effizientere Zugangsbeschränkung. Hier kommt die Biometrie ins Spiel: Biometrische Merkmale sind maximal fälschungssicher. Daher brauchen sich die Nutzer entsprechender Autorisierungssysteme und -technologien auch keine Gedanken über Wechsel und Updates machen. Aus gutem Grund verfügen immer mehr mobile Rechner über Fingerabdruck-Scanner.

Handvenenscan per Infrarot

Die Fingerabdruck-Erkennung ist jedoch bei weitem nicht das letzte Wort in Sachen Sicherheit. Denn wo selbst ein Fingerabdruck – zumindest theoretisch – noch gefälscht oder imitiert werden kann, ist das bei einem anderen individuellen Merkmal schlicht unmöglich: dem Muster der Handvenen. Fujitsu hat ein Verfahren mit der Bezeichnung PalmSecure entwickelt, das die Venen der Handfläche als Identifikationsmerkmal nutzt. Dazu braucht der Anwender nicht einmal den Laptop – oder jedes andere Gerät, das die Technologie nutzt – zu berühren. Beim Scanvorgang per Infrarotlicht absorbiert das sauerstoffarme Hämoglobin in den Handvenen das Licht. Dadurch erscheinen die Venen als schwarzes Muster. Dieses Muster wird nach erstmaliger Erfassung als Vorlage für jede folgende Authentifizierung verschlüsselt abgelegt. Dabei erkennt der Sensor das Muster nur, wenn das Hämoglobin aktiv in den Handvenen fließt. Das heißt: Der Nutzer muss physisch anwesend sein.

Ein Venenmuster zu fälschen, ist so gut wie unmöglich. Zudem bietet das System eine ausgesprochen niedrige Fehlerrate. Das macht PalmSecure um das Zehnfache sicherer als einen Iris-Scan – und sogar um das Hundertfache zuverlässiger als die Authentifizierung über einen Fingerabdruck. Dabei spielt es auch keine Rolle, wenn sich mehrere Mitarbeiter eine Celsius H730 teilen. Dann werden die Venenmuster der betreffenden Nutzer mit unterschiedlichen User Accounts auf dem Rechner verknüpft.

Zusammenspiel der Technologien

Leistungsfähigkeit und Sicherheit sind nicht zu trennen, wenn es um den Einsatz mobiler Workstations im professionellen Bereich geht. Biometrische Sicherheitsverfahren gewährleisten den erforderlichen Schutz sensibler Daten auf Laptops. Noch besser ist es natürlich, wenn ein Gerät mehrere Sicherheitstechnologien miteinander kombinieren kann. Fujitsu ergänzt PalmSecure mit weiteren Komponenten wie Fujitsu Advanced Theft Protection und Trusted Platform Module (TPM) – ein Rundum-Schutz, der Systeme wie den CELSIUS H730 zu einem Hochsicherheitstrakt für Daten macht. *(anm)* ■