Vorsicht ist besser als Nachsicht.

Rundum-Schutz Ihrer Geräte mit Lenovo.

Jede Minute wird ein Notebook gestohlen. Deshalb sollten Sie jedoch nicht die Mobilität Ihrer Mitarbeiter einschränken. Sie können potenzielle Risiken mit einer **robusten Gerätesicherheit minimieren.**

Sie sind der Meinung, Ihr Gerät ist sicher? Von wegen.

In Hinblick auf die Netzwerksicherheit sind die Geräte am anfälligsten für Bedrohungen.

Alle **53 Sekunden** wird ein Notebook gestohlen.

52 % der Geräte werden aus Büros gestohlen.

80 % der Kosten eines verlorenen Notebooks sind der Datensicherheitsverletzung zuzuschreiben.

Nichts zu unternehmen kann teuer werden.

Der Verlust eines Geräts ist verheerend, wenn es für den Zugriff auf vertrauliche Daten verwendet wurde. Nicht nur für den Benutzer, sondern auch für Ihr Unternehmen.

- November 2016: EMC und Hartford Hospital zahlten eine Strafe von 90.000 US-Dollar aufgrund des Diebstahls eines Notebooks mit Daten von fast 9.000 Personen.
- Mitte 2012: Cancer Care Group zahlte eine Strafe von 750.000 US-Dollar aufgrund des Diebstahls eines Notebooks mit personenbezogenen Daten von 55.000 aktuellen und ehemaligen Patienten.
- 2006: Nationwide musste eine Strafe von 980.000 £ aufgrund des Diebstahls eines nicht verschlüsselten Notebooks zahlen, das die personenbezogenen Daten von 11 Millionen Sparern enthielt.

360° -Sicherheitsstrategie von Lenovo

BENUTZERZUGRIFFS-STEUERUNG

Beschränken Sie den PC-Zugriff mit den folgenden Features ausschließlich auf autorisierte Personen:

Multifaktor-Authentifizierung

Die biometrische Fingerabdruckerkennung von Lenovo gewährleistet einfaches Zugriffsmanagement und robuste Sicherheit. Als führender Anbieter im Bereich Multifaktor-Authentifizierung bietet Lenovo außerdem folgende Leistungsmerkmale in seinen Geräten:

- Mithilfe der Technologie des **„Match on Chip (MoC)"-Lesegeräts für Fingerabdrücke** erfolgt die Speicherung biometrischer Anmeldeinformationen auf einem separaten Chip, der fast unmöglich zu hacken ist.
- **Intel® Authenticate** schützt zusätzlich Ihre Identität und Daten.

SmartCard-Zugriff

Anmeldeinformationen werden auf fälschungssicheren Karten gespeichert. Es sind keine Kennwörter nötig.

Near Field Communication (NFC)

Funkübertragungstechnologien wie Bluetooth oder WLAN mit Tags verhindern das Eindringen in ein Gerät.

IR-Kamera mit Windows Hello

Mit Windows Hello vereinfacht und sichert die optionale IR-Kamera auf ausgewählten Geräten das Anmeldeverfahren. Bei der Windows Hello-Gesichtsauthentifizierung wird eine Kamera zum Entsperren des Geräts verwendet, die speziell für Nahinfrarotaufnahmen (IR) konfiguriert ist.

Technologievorstellung
Das „Match on Chip"-Lesegerät für Fingerabdrücke (MoC FPR) von Lenovo zählt zu den sichersten Fingerabdrucktechnologien auf einem PC

Technologievorstellung
Die Abdeckung der Kameralinse des Lenovo ThinkPad ist eine mechanische Webcam-Abdeckung, die Benutzer bei Anrufen öffnen und ansonsten geschlossen lassen können.

SCHUTZ DER ANSCHLÜSSE UND PHYSISCHE SICHERUNG

Vermeiden Sie Datendiebstahl über USB oder andere Anschlüsse an Firmen-PCs durch folgende Features:

Abdeckung der Kameralinse

Die eingebaute Abdeckung der Kameralinse sorgt für Privatsphäre.

Kensington®-Kabelverriegelung

Die Kensington®-Kabelverriegelung gehört zur Standardausrüstung von Lenovo PCs. Kunden können damit den physischen Gerätezugriff im Büro absichern.

Lenovo ThinkPad Ultra Dock

Das Lenovo ThinkPad Ultra Dock verfügt über ein Sicherheitsschloss, mit dem Sie das Gerät und Ihre Andockstation bequem am Tisch befestigen und absperren können. Dafür ist nur ein Schlüssel erforderlich.

DATENSICHERHEIT

Vermeiden Sie Datendiebstahl und -verlust durch folgende Features:

Bessere Verwaltung und Kontrolle

Erleben Sie Pro SSD Integration mit Intel® Remote Secure Erase von Intel® Active Management Technology (Intel® AMT).

Fast Identity Online (FIDO)

Die FIDO-Authentifizierung steht in Verbindung mit Onlineanmeldedaten, wenn Benutzer sich bei internen oder externen Websites anmelden oder Onlinezahlungen tätigen.

Discrete Trusted Platform Module (dTPM)

Der in Lenovo ThinkPad Geräten eingebettete dTPM 2.0-Chip aktiviert und speichert eindeutige, für das Hostsystem spezifische RSA-Verschlüsselungsschlüssel zur Hardware-Authentifizierung.

Integrierte Mobilgeräteverwaltung

Mit der Unterstützung von Mobile Device Management (MDM) von Windows 10 können Sie cloudbasierte Verwaltungsdienste* verwenden, um Geschäfts- oder Privatgeräte zu steuern.

*separat erhältlich

Technologievorstellung
Der dTPM 2.0-Chip verschlüsselt automatisch die Benutzerdaten auf dem PC.

Quelle:
https://www.pcworld.com/article/3021316/security/why-stolen-laptops-still-cause-data-breaches-and-whats-being-done-to-stop-them.html
https://www.digicert.com/blog/45-percent-healthcare-breaches-occur-on-laptops/
https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/

Mit Lenovo haben Sie die Gewissheit, dass Ihre Geräte und Daten stets geschützt sind.

Weitere Informationen finden Sie unter www.lenovo.com

Lenovo

Intel® Core™ Prozessoren

www.lenovo.com