Keylogger

Als Keylogger wird Hardware und Software bezeichnet, mit der die Tastatureingaben eines Computernutzers erfasst, gespeichert und unbemerkt übermittelt werden. So kann es zum Missbrauch von sensiblen Daten wie PINs und Passwörtern kommen.

Unterschiedliche Keylogger

Software-Keylogger speichern die Tastatureingaben entweder auf der Festplatte des PCs oder übermitteln sie über das Internet. Sie arbeiten für den Computernutzer nicht sichtbar im Hintergrund. Anders ist das bei Hardware-Keyloggern. Sie werden, etwa in Form eines USB-Sticks, zwischen Tastatur und Computer gesteckt. Das Installieren von Keyloggern und somit das Ausspähen von Daten ist ohne Kenntnis beziehungsweise Zustimmung deren Nutzer laut Paragraph 202a des Strafgesetzbuchs strafbar.

Funktionen der Keylogger

- Aufzeichnen sämtlicher Tastatureingaben
- Speichern des Browserverlaufs, auch wenn dieser gelöscht wurde
- Screenshots des Desktops
- Protokollieren von Chats und Mails

Schutz vor Keyloggern

Hardware-Keylogger sind einfach zu finden, indem man die Tastatur und das Verbindungskabel nach fremden Elementen absucht. Bei der Eingabe von Passwörtern kann man zum Beispiel auch die „virtuelle Tatstatur“ verwenden. Sie schützt vor Hardware-Keyloggern. Man findet die virtuelle Tastatur, indem man am Computer unten links auf das Startmenü klickt, in das Suchfeld "Bildschirmtastatur" eingibt und das Ergebnis dann anklickt. Vor Software-Keyloggern schützen Anti-Spyware-Programme und ein aktueller Virenscanner.

Siehe auch:
Internet Protocol (IP)

Zurück