Logger

Logger bezeichnen Geräte, mit denen etwas 'geloggt', also mitgeschnitten werden kann. Für uns hier sind zwei Arten von Logger relevant: Keylogger und Screenlogger.

Keylogger

Keylogger sind Geräte, die im Grunde sämtliche Tasteneinschläge auf eurer Tastatur mitschneiden. Dafür sitzen sie zwischen Tastatur und Computer und sehen aus wie normale USB-Adapter:

Keylogger neben Tastatur

Keylogger zwischen Laptop und Tastatur

Sie können über Funk/WLAN/LTE in Echtzeit jeden einzelnen Tasteneinschlag zu einem Angreifer senden. Das Problem daran ist offensichtlich.

Diese Keylogger sind für sehr kleines Geld zu haben und einfach zu besorgen, sodass ihre Anwendung auch für Amateure sehr simpel ist!

Es gibt sogar Keylogger die wie ein ganz normales Kabel aussehen, siehe z.B. das O.MG Cable.

Fortgeschrittenere Angreifer (zB. Behörden) können auch Keylogger in den Tastaturen selbst verbauen, indem sie die Tastatur aufschrauben und eine kleine Keylogger-Platine an der Elektronik der Tastatur direkt verbauen. Oder sie tauschen die Tastatur einfach durch eine manipulierte aus. Das würde dann allein am USB-Port natürlich nicht auffallen.

Screenlogger

Screenlogger funktionieren nach dem gleichen Prinzip wie Keylogger. Ein Adapter-ähnliches Gerät wird zwischen Display und PC gesteckt (je nach verwendetem Anschluss: VGA, HDMI, DisplayPort,...) und kann dann die gesamte Bildübertragung mitschneiden und über Funk/WLAN/LTE an den Angreifer senden.

Warnung
• vor öffentlich zugänglichen PC's

- anderen PC's die nicht immer unter Beobachtung sind (das eigene Büro zB.)

Es sei noch erwähnt, dass mit "Key-" bzw. "Screenlogger" auch Software-Logger gemeint sein können. Dass sind dann aber nichts anderes als Viren und beschreiben eine völlig andere Bedrohung als diese hier.

Version #1
Erstellt: 25 Januar 2025 10:39:24 von ESC-IT Migration Bot
Zuletzt aktualisiert: 25 Januar 2025 10:39:25 von ESC-IT Migration Bot