

Das Projekt kann man als tragbare Blackbox betrachten, die Datenträger analysiert, mit sofortiger Erkennung des Risikos des Geräts. Im Detail besteht das Projekt aus einem Raspberry Pi 3B+ mit Touch-Display, das Dateien auf USB-Sticks und anderen Speichermedien auf ihre Gefährlichkeit untersuchen kann. Abhängig von den gefundenen Daten werden auf dem dedizierten Display mögliche Aktionen und Informationen angezeigt: Als böartig gemeldete Dateien können in Quarantäne gestellt werden (in einem dedizierten Ordner, damit sie nicht ausgeführt werden), in einen anderen Ordner verschoben werden (um einfacher vom Benutzer auf einem separaten Gerät exportiert zu werden) oder gelöscht werden, außerdem könnte es einen Risikoindex des analysierten Geräts geben. Darüber hinaus besteht die Idee darin, ein angepasstes Betriebssystem zu erstellen, um die Leistung zu steigern und den Raspberry Pi nicht zu überlasten, und durch ein in Python geschriebenes Programm ein dediziertes Antivirus für Linux zu erstellen. Das System kann dann mit WLAN verbunden werden, um auf eine öffentliche DB (z. B. <https://www.virustotal.com/>) zu verweisen, um die verwalteten Dateien analysieren zu können. Darüber hinaus wird aus Gründen der DSGVO / Datenschutz die Notwendigkeit für den Benutzer, der diese Lösung verwendet, den Warnhinweis zur Verwaltung der analysierten Daten zu akzeptieren, auf dem Touchscreen-Display integriert (was in keinem Fall auf dem System gespeichert würde, aber auf dem Speichergerät belassen). Das Endergebnis, um zu verstehen, ob das Gerät die vom Unternehmen geforderte Konformität erfüllt, ergibt sich aus der auf dem Display angezeigten Risikostufe. Auf der Grundlage des Ergebnisses kann das Unternehmen daher entscheiden, ob das vom Lieferanten / Kollegen vorgeschlagene Speichergerät verwendet wird oder nicht. Das Projekt ist aber nicht als fertiges Produkt anzusehen, sondern als POC (Proof of Concept).