TeleTrusT
Pioneers in IT security.

TeleTrusT-interner Workshop

Berlin, 05./06.07.2018

Höhere Sicherheit durch KI-gestützte Authentifizierung

Sascha Dubbel, Senior Security Engineer, T.I.S.P.

Cylance Deutschland GmbH

Authentifizierung bisher

- Großteil von Benutzer-Authentifizierungen ist Benutzername/Passwort-basiert
- Richtlinien zur Komplexität nicht standardisiert
- Multifaktor-Authentifizierung ergänzt vorhandene Verfahren
- Neue Single-Sign-on-Verfahren (SSO) haben ein gute Nutzerakzeptanz aber auch Risiken?

Die Schwächen klassischer Verfahren

- Erste Mehrfaktor-Authentifizierungen waren umständlich zu betreiben (Hardware-Token sind Verwaltungs- und Kostenintensiv)
- Alte Anwendungen bieten häufig keine alternativen Schnittstellen (100 Passwörter für 100 Anwendungen)
- SSO zum Teil schwach gegen bestimmte Angriffe (man-in-the-browser, man-in-the-middle etc.),
- Eine erfolgreiche Authentifizierungssequenz beweist in der Regel nicht ausreichend die Identität einer Person

Künstliche Intelligenz eröffnet neue Möglichkeiten

- kontinuierliche Validierung der Benutzeridentität ist wünschenswert.
- KI-Modelle können zuverlässig lokal am Endpunkt eines Benutzers trainiert werden (Verhalten, Nutzung, ergonomische Muster)
- fortlaufende Optimierung der Selektion relevanter Merkmale (Datenvermeidung) und Mechanismen zur Vermeidung unnötiger Re-Authentifizierungen
- Datenschutz muss beachtet werden -> lokale Verfahren sinnvoll

Ideen zur Anwendung von KI in der Authentisierung

- Features
  - Bewegung
  - Dynamik
  - Zeit
  - Ort
  - ...
- Herausforderungen
  - Autarkie
  - Einfachheit
  - Datenschutz/-vermeidung
  - Hohe Genauigkeit
  - Resistenz gegen Manipulation
  - ...