ERSTE GROUP

Robotic Process Automation
–
Risken und abzusichernde Felder

C. Koza, 17. April 2018
Group IT Audit, Erste Group Bank AG

Agenda

ERSTE GROUP

Problembeschreibung

- Maschinen-zu-Maschinen – Kommunikation kennen wir schon lange
- Eigenschaften Software Robots
- Abgeleitete Risiken und notwendige Mitigationen

Gedanken zu Mitigationen

- Roboter von Menschen unterscheiden können
- Missbrauch von „Roboter-Credentials“ verhindern
- Robot-Anwendungen sind ganz normale SW-Anwendungen

Problembeschreibung

ERSTE GROUP

- Maschinen-zu-Maschinen – Kommunikation kennen wir schon lange
  - File-Schnittstellen, rpc, Client-Server – Systeme (z.B.: CORBA)
  - Authentifizierung über User-Passwort, Zertifikate, …

- Eigenschaften Software Robots
  - Verwenden Schittstellen (z.B.: Masken), die für menschliche Benutzer gebaut wurden,
    - Um Kosten für Entwicklungen zu vermeiden,
    - Um nicht in alte Software eingreifen zu müssen oder
    - Weil umfangreiche Einmalaktion (z.B. Bereinigung) stattfinden soll
  - Arbeiten deshalb mit Benutzer-Credentials die auch Menschen verwenden könnten,
    - Haben oft auch umfangreiche Berechtigungen
  - Aktivitäten werden mit den selben Mechanismen gelogged, nachvollzogen, wie bei menschlichen Benutzern

- Abgeleitete Risiken und notwendige Mitigationen
  - Aktivitäten von Robotern von jenen von Menschen unterscheiden können
  - Missbrauch von „Roboter-Credentials“ durch Menschen verhindern
  - Robot-Anwendungen sind ganz normale SW-Entwicklung

Gedanken zu Mitigationen

ERSTE GROUP

- Roboter von Menschen unterscheiden können
  - Erkennbarkeit durch geeignete Namensgebung
    - User-Name,
    - Personalnummer,
  - Zuordnung zu einer „Roboter-OE“
  - Beschränkung Gültigkeit auf spezifischen „Roboter-Arbeitsplatz“

Institut	OE	Bezeichnung	Telefon	Kurzinfo	EMailSMS
ErsteGroup	0196	RobotUser1 Gordon		externer Mitarbeiter	
ErsteGroup	0196	RobotUser1 Romedius		externer Mitarbeiter	
ErsteGroup	0196	RobotUser2 Roberta		externer Mitarbeiter	

Gedanken zu Mitigationen (cont.)

ERSTE GROUP

- Missbrauch von „Roboter-Credentials“ verhindern
  - Passwort nur gültig während Session,
    Nur Roboter kennt das Passwort,
    - z.B.: Rest am Beginn und nach Ende der Session,
  - Nach dem Test arbeitet der Roboter in der „Produktion“ nur mehr ohne Bildschirm und Tastatur,
    - z.B.: auf einem virtual Client der keinen „Reader“ erlaubt
  - Festlegen/Beschränken der Berechtigungen/Rollen in einem Ausmaß, dass der Account für Menschen unbrauchbar wird,
  - Ausreichendes Logging durch den Software Robot
    - Damit können Roboter-Transaktionen klar dem Roboter zugeordnet werden

Gedanken zu Mitigationen (cont.)

ERSTE GROUP

- Robot-Anwendungen sind ganz normale SW-Anwendungen
  - Ordnungsgemäße Entwicklung und Betrieb muss sichergestellt werden!

- SW-Lifecycle muss eingehalten werden
  - Was soll erreicht werden? (Anforderung)
  - Wie soll es erreicht werden? (Design)
  - Wurde gewünschte Funktion erfüllt? (Tests und Testdokumentation)

- Härten der Systeme
  - Um Missbrauch durch menschliche Benutzer zu vermeiden
  - Um Missbrauch, durch Cyber-Attacken zu vermeiden

Gedanken zu Mitigationen (cont.)

ERSTE GROUP

- IT-Prozesse müssen wie bei allen Anwendungen angewendet werden!
  - Incidents-,
  - Change- und
  - Test-Management,
    - speziell auch Gesamtintegrationstests (Maskenänderungen)!

- Robots in der Datenfluß- und Ablaufdokumentation nicht vergessen
  - Robots sind nicht unbedingt in der klassischen Ablaufsteuerung enthalten,
  - Sicherstellen, dass Aubläufe von Robots in der Gesamtbetrachtung nicht vergessen werden!

Kontakt

ERSTE GROUP

Dipl. Ing. Dr. Christian Koza, CISA, CRISC
Head Audit IT
Erste Group Bank AG
OE 0361 / Audit IT

A-1100 Wien, Am Belvedere 1
Phone: +43 5 0100 / 12752
mailto: Christian.Koza@erstegroup.com