ATM-Sec

Air Traffic Management - Cyber Security Analyse

Programm / Ausschreibung	TAKE OFF, TAKE OFF, TAKEOFF Ausschreibung 2017	**Status**	abgeschlossen
Projektstart	01.11.2018	**Projektende**	31.01.2021
Zeitraum	2018 - 2021	**Projektlaufzeit**	27 Monate
Keywords	ATM, Cyber Security, Briefing System		

Projektbeschreibung

Anlass dieses Projekts ist die im Jahr 2018 in Kraft tretende EU Richtlinie zur Netz- und Informationssicherheit, kurz NIS Direktive [01]. Schwerpunkt der Forschungsaktivität liegt auf deren konkreter Auswirkung auf Systeme im Bereich der Flugsicherung.
Im aktuellen Air Traffic Management (ATM) kommen für die Flugvorbereitung moderne Internet Briefing Systeme, kurz IBS, zum Einsatz. Diese Systeme selbst können nach NIS Qualifizierung als unkritisch betrachtet werden, bieten jedoch eine Vielzahl an Schnittstellen zu anderen Systemen, die einer kritischen Infrastruktur angehören.
Das IBS soll speziellen Cyber-Angriffen unterzogen werden. Dafür soll ein Testbed aufgebaut werden, das neben dem Hauptsystem auch über diverse Schnittstellen verfügt, die die unterschiedlichen Domänen (kritisch/unkritisch) simulieren. Auch für an die kritische Infrastruktur angrenzende Systeme, sind folgende Aspekte interessant und werden durch das Projekt beleuchtet: Grad der Härtung, Unterstützung eines sicheren Betriebes, Mögliche Angriffskette, ATM Security Methoden im Verhältnis zur NIS Direktive, Beeinflussbarkeit eines Systems der Kritischen Infrastruktur durch ein angrenzendes.
Während des Projekts werden Szenarien und Use Cases ausgearbeitet, die einer Risikoanalyse unterzogen werden, welche für die anschließenden Testverfahren (Statische und Dynamische Security Analyse) als Grundlage dienen.
Die Erkenntnisse fließen zurück in die System- und Softwareentwicklung. Das Ziel ist die Überarbeitung und Verbesserung der Security Aspekte des bestehenden Softwareentwicklungsprozesses, welcher u.a. für das Internet Briefing System zum Einsatz kommt.
Dabei soll auch ein Fokus auf das Toolset gelegt werden, um das Security-Konzept des Softwareentwicklungsprozesses auch für andere, ähnliche Systeme zur Anwendung zu bringen. Abschließend wird auch ein Betriebskonzept für den sicheren Umgang mit dem System im Umfeld der kritischen Infrastruktur erarbeitet.

Abstract

The basic motivation for this project is the EU Network and Information Security Directive, or NIS Directive [01], which will enter into force in 2018. The focus of the current research activity is on the NIS Directives impact on systems in the field of Air Traffic Management (ATM).
Current ATM uses and future ATM mandates modern Internet briefing systems (IBS) in the flight preparation phase. These

systems can be considered non-critical according to NIS qualification, but they offer a variety of interfaces to other systems that belong to a critical infrastructure.
During the project, selected IBS will be subjected to specifically designed cyber-attacks. For this purpose, the project team will set up a testbed which, in addition to the main system, also has various interfaces which simulate the different domains (critical / uncritical).
The following aspects are interesting for systems adjacent to critical infrastructure and are examined by the project: degree of hardening, support of secure operation, possible attack chains, ATM security methods in relation to the NIS directive and vulnerability of a system of critical infrastructure by means of an adjacent node.
Moreover, there will be scenarios and cases of use, which will serve as the basis for a risk analysis, which will guide the subsequent development and execution of the respective test procedures (static and dynamic security analysis).
The findings will flow back into system and software development. The main project goal is to optimize and enhance the security aspects of currently used software development processes, which will be applied, among others, to internet briefing system development.
The toolset established in the project may also be integrated in the general software development environments for similar systems.
Finally, the project intends to develop a concept for guiding the secure operation of a system in the critical infrastructure domain.

Projektkoordinator

- FH JOANNEUM Gesellschaft mbH

Projektpartner

- FREQUENTIS AG