SUCCESS STORY

infodas®
COLOGNE IT SOLUTIONS & SERVICES

RSGate®

Das BSI zugelassene Sicherheitsgateway zur Informationsflusskontrolle

Sicherer Informationstransfer zwischen roten und schwarzen Domänen

Kontrollierter Informationsfluss in der Flugsicherung

Erfolgreicher Einsatz des von INFODAS GmbH entwickelten und vom Bundesamt für Sicherheit in der Informationstechnik (BSI) bis GEHEIM zugelassenen RSGate® *(Rot/Schwarz-Gateway) für das Flugsicherungs- und Informationssystem der Bundeswehr*

Neben dem Einsatz eines RSGate® für die Teilstreitkraft Marine konnten wir uns somit auch erfolgreich in der Luftwaffe mit der am 27.01.2009 vom BSI an uns vergebenen Einzelzulassung BSI-EZ-VSA-0014-2008 positionieren.

Motivation: In fast allen Bereichen der Bundeswehr, der öffentlichen Verwaltung, der geheimschutzbetreuten Industrie, aber auch der Sicherheitsbehörden wie Polizei und Nachrichtendienste ist die Behandlung von eingestufter Information ein wichtiges und kritisches Thema.

Durch den zunehmenden Grad der Vernetzung der IT-Systeme hat sich das Verständnis vom Umgang mit eingestuften Informationen auf den Umgang mit eingestuften Systemen, so genannte *rote Systeme,* erweitert. Diese verarbeiten, speichern oder leiten eingestufte Informationen weiter. Bis vor kurzem war ein möglicher Abfluss von eingestuften Daten weniger kritisch, da diese Systeme über keinerlei Verbindung zu niedriger eingestuften Systemen verfügten. Lediglich Verbindungen zu gleichermaßen eingestuften Systemen wurden realisiert, was zum Aufbau sog. *roter Domänen* führte. Vor dem Hintergrund einer immer weiter steigenden vernetzten Operationsführung (NetOpFü) gewinnt die Integration aller Informationssysteme zunehmend an Bedeutung.

Die Notwendigkeit eines Sicherheitsgateways, mit dem Daten zwischen höher eingestuften *roten* und niedriger eingestuften *schwarzen Bereichen* und umgekehrt transferiert werden können, wird immer deutlicher. Ein zulässiger *Rot-Schwarz-Übergang* erfordert eine inhaltliche Prüfung der zu übertragenen Dokumente und Daten im Rahmen einer gezielten und nachweisbaren Informationsflusskontrolle. Dies können herkömmlichen Firewall-Systeme nicht leisten.

Hintergrund: Die Realisierung eines zuverlässigen und gesicherten Informationstransfers zwischen roten und schwarzen Domänen erfordert die Replikation der Datenbank des FSInfoSysBw (schwarz) in den Sicherheitsbereich des FüInfoSysLw (rot). Ziel dieser Lösung ist die Bereitstellung der Flugsicherungsinformationen für rote Systeme, die somit Zugriff auf ein Replikat dieser Informationen innerhalb roter Netze erhalten. Im Auftrag der Avitech AG konzipierte und realisierte INFODAS GmbH hierfür auf Basis des Produktes RSGate® eine geeignete Lösung. Diese stellt neben der erforderlichen Replikation der „Master"-Datenbank des FSInfoSysBw (schwarz) auf einen Datenbankserver im Sicherheitsbereich des FüInfoSysLw (rot) ebenfalls sicher, dass keine Informationen aus dem roten Bereich unkontrolliert in den schwarzen Bereich zurückfließen können.

Problemfelder bei der Rot/Schwarz-Replikation der Datenbanken:

- Aus den **Schutzanforderungen** heraus ist zuverlässig zu verhindern, dass *rote Daten* unkontrolliert oder unberechtigt die *rote Domäne* verlassen. Ein revisionssicherer Prozess muss garantieren, dass nur Daten, die explizit freigegeben wurden die *rote Domäne* verlassen. Andererseits ist sicherzustellen, dass Daten, die aus der *schwarzen* in die *rote Domäne* transferiert werden, zuverlässig nach Viren, aktiven Inhalten und Schad-Software gefiltert werden, um so das sensible rote Netz vor schädlichem Code zu schützen.
- Die **Kommunikationsanforderungen** beziehen sich auf die Unterstützung der TCP/IP-Protokollfamilie. Das RSGate® bietet hierfür eine Datenübertragung von E-Mails mit Datei-Anhängen auf der Basis von SMTP.
- Die **Performanceanforderungen** der Einsatzumgebungen sind unterschiedlich, von sehr kompakt mit geringem Durchsatz bis zu einem hochskalierbaren Cluster und sollen durch konfigurierbar ausgelegte Systeme unterstützt werden. Da zurzeit keine sehr hohen *Verfügbarkeitsanforderungen* und keine Performance-Engpässe wie z. B. 24 Std.-Betrieb, erkennbar sind, ist eine Clusterlösung nicht erforderlich. Aufgrund des hohen Datenaufkommens wird die Funktionalität der manuellen Freigaben durch E-Mails ausschließlich für Administrationszwecke genutzt.

Die Lösung und ihre Funktionalitäten:

- Einsatz/Installation des nach *ITSEC E3/hoch* evaluierten RSGate® am Domänenübergang
- Sicherstellung der Kontrolle des Inhalts der übertragenen Daten durch eine digitale Signatur mit anschließender Verifikation durch einen zentralen Sicherheitsfilter
- Replizieren von Datenbanken durch Übergabe von Replikationsdaten von *Schwarz* nach *Rot*
- Dateiübertragung in Form von E-Mail-Anhängen (SMTP)
- Signatur schwarzer Daten (Transaktionskennungen) durch den Sicherheitsfilter am Netzübergang
- Übergabe der Replikationsdaten und signierter Transaktionskennung an den roten Datenbankserver
- Übernahme von XML-Dokumenten mit Statusinformationen sowie der ursprünglichen, durch die Signatur unveränderbaren Transaktionskennung sowie die Prüfung/Signatur zulässiger Antworten mittels XML- Schemata
- Prüfung der Integrität der Dokumente durch den Sicherheitsfilter
- Schutz vor Angriffen aus dem schwarzen Netz durch ein integriertes GeNUGate®-Firewallsystem (zertifiziert nach CC EAL 4+)
- integrierte Funktionen zur sicheren Administration der Komponenten

Über die INFODAS GmbH

INFODAS gehört zu den innovativen deutschen mittelständischen Systemhäusern für IT-Sicherheits- und Risikomanagement. Neben Konzeption, Entwicklung, Integration und Aufbau von evaluierten IT-Sicherheitslösungen führen die von BSI-lizenzierten ISO 27001- und IT-Grundschutz-Auditoren geleiteten Projektteams der INFODAS ganzheitliche IT-Sicherheitsberatungen mit Hilfe des Werkzeugs SAVe® durch. Sie konzipieren bzw. auditieren IT-Sicherheitsmanagementsysteme gemäß ISO 27001, BSI-Standard 100-1 bzw. ZDv 54/100. INFODAS entwickelt geeignete Notfallvorsorge-Programme, gestaltet und überprüft den Datenschutz und stellt externe Datenschutzbeauftragte zur Verfügung.

INFODAS - Gesellschaft für Systementwicklung und Informationsverarbeitung mbH
Rhonestr. 2
50765 Köln
Telefon (0221) 709 12 - 0
Fax (0221) 709 12 - 55
infodas@infodas.de
www.infodas.de