Mit Smard-Cards um die Welt

Die Einbindung von Smart-Card-Authentifizierung in bestehende Infrastrukturen ist nicht trivial – vor allem, wenn dazu noch verschiedene Verzeichnisdienste in heterogenen Netzen zum Einsatz kommen. Das Deutsche Zentrum für Luft- und Raumfahrt hat dieses Problem mit einer Zwischenschicht gelöst.

Sicherheit ist eine Grundtugend der IT. Umso mehr, wenn im Falle unbefugten Zugriffs auf die Systeme Menschenleben und hohe Sachwerte in Gefahr sind. Entsprechend aufwändig ist das Sicherheitskonzept im Raumfahrtkontrollzentrum des Deutschen Zentrums für Luft- und Raumfahrt in Oberpfaffenhofen. Hier wird rund um die Uhr das Columbus-Modul der internationalen Raumstation ISS gesteuert.

Wie in vielen anderen Unternehmen mit hohen Sicherheitsanforderungen basiert das Konzept des DLR auf getrennten Netzwerken unterschiedlicher Schutzstufen, die keine Berührungspunkte haben: Im so genannten Ops-Netz findet die eigentliche Steuerung des Forschungsmoduls im Erdorbit statt, darunter die Kontrolle der lebenserhaltenden Systeme. Hier gelten strengste Sicherheitsrichtlinien, wie sie zum Beispiel auch in Banken üblich sind, damit kein Unbefugter Kommandos an die ISS absetzen kann. Parallel dazu existiert das Netz „Ops Support“. In diesem Segment laufen verschiedene Hilfsmittel für die Flight Controller, etwa ein Tool zur minutiösen Tagesplanung der ISS-Besatzung. Die Sicherheitsansprüche hier sind mit den Standards in unternehmenskritischen Bereichen anderer Industrien vergleichbar: Ein Fehler im System oder eine Manipulation der IT von außen könnte gravierende Störungen im Ablauf der Raummission und nicht zuletzt

hohe Kosten zur Folge haben. Die geringsten Sicherheitsansprüche bestehen im Office-Netz. Nur in diesem Teil der Infrastruktur kann auf das Internet zugegriffen werden, Office-Programme und E-Mail dominieren dieses Segment. Den Betrieb der IT hat das DLR in weiten Teilen an verschiedene externe Dienstleister ausgelagert.

Für das Ops-Support-Netzwerk ist die auf dem DLR-Gelände ansässige INSYEN AG zuständig. Alle Vorgaben zur IT-Gestaltung werden von der europäischen Raumfahrtbehörde ESA aufgestellt, in deren Auftrag das DLR das Columbus-Modul steuert. So sieht das ESA-Reglement zum Beispiel vor, dass die Benutzerauthentifizierung ausschließlich über einen zentralen LDAP (Lightwight Directory Access Protocol)-Server abläuft. Im hochkritischen Ops-Netz ist zudem die Anmeldung über Smart-Cards vorgeschrieben – eine Authentifizierungsmethode, die auch auf das Ops-Support-Netz ausgeweitet werden musste. Das grundsätzliche Problem dabei erläutert Harald Stößner, Betreuer des Ops-Support-Netzes: „Das Ops-Support-Netz ist eine gewachsene Windows-Domäne. LDAP als führendes System hier mit den Windows-Bordmitteln einzubinden hätte einen enormen Aufwand und viel manuelles Eingreifen erfordert.“ Auch die Integration der Smart-Cards wäre sehr komplex gewesen. „Wir haben deswegen eine Lösung gesucht, die alle drei Welten miteinander verbinden kann – das Active Directory der Windows-Domäne, die zentralen LDAP-Services und die Authentifizierung über Smart-Cards“, ergänzt Jürgen Fein, zuständig für die Abläufe im DLR-Kontrollzentrum, die Ausgangslage. Ein technisches Grundproblem dabei ist, dass Active Directory normalerweise der Master innerhalb eine Domäne sein will. Beim DLR jedoch bildet laut ESA-Vorgabe LDAP den Master, der Windows-Domain-Controller im Ops-Support-Subsystem muss in die zweite Reihe treten.

„Das bestehende Active Directory auszutauschen war keine sinnvolle

Option“, so Fein. „In der Windows-Domäne laufen zum Teil wichtige Tools der NASA, die für Windows konzipiert wurden und diese Infrastruktur voraussetzen.“ Die Auswahl und Evaluierung einer geeigneten Lösungen als Brücke zwischen den unterschiedlichen Systemwelten konnte laut Fein sehr sorgfältig angegangen werden, da die Vorgaben frühzeitig bekannt waren. „Viel Auswahl gab es nicht“, erinnert sich Stößner. „Wir haben nur ein Produkt gefunden, das allen unseren Anforderungen gerecht wird.“ Entsprechend fiel die Entscheidung zu Gunsten der Lösung „SignOn Gate“ der Wiener Comtarsia IT Services GmbH.

Zur Evaluierung der Lösung wurde zunächst ein Backup-Kontrollraum damit ausgestattet. Hier ist das DLR-Kontrollzentrum in der glücklichen Lage, neue IT-Lösungen während der Aus- und Weiterbildung der Flight Controller in praxisnahen Simulationen des Normalbetriebs testen zu können. Dabei zeigte sich, wo die ausgewählte Lösung noch an den individuellen Bedarf anzupassen war. Dazu zählt zum Beispiel der Einsatz mehrerer PCs an jedem Arbeitsplatz: Durch die strikte Trennung der verschiedenen Netze arbeiten die Flight Controller der DLR mit drei Rechnern, von denen jeder einem der drei Netze fest zugeordnet ist. Normalerweise wird bei der Authentifizierung mittels Smard-Cart ein Benutzer abgemeldet oder der PC gesperrt, wenn die Karte aus dem Lesegerät entfernt wird. Im Kontrollzentrum durfte das aber nicht passieren – die Benutzer melden sich mit einer einzigen Karte an allen Maschinen an. Diese Karte dient zudem auch als Zugangskontrolle zum Flight-Control-Raum und zu den Gebäuden. „Innerhalb unseres Sicherheitskontexts mit strengen, mehrstufigen Zugangskontrollen und physikalisch getrennten Netzen können wir es tolerieren, dass ein Benutzer im Ops-Support-Netz angemeldet bleibt, auch wenn die Smart-Card abgezogen ist“, so Fein. „Im hochsicheren Ops-Netz, in dem die Steuerung des Columbus-Moduls läuft, wäre das hingegen nicht möglich.“ Comtarsia realisierte die entsprechenden

Funktionen.

Eine weitere Hürde war die hoch heterogene Umgebung: Smart-Cards werden in zwei Subsystemen – Ops und Ops-Support – eingesetzt. Jedoch kommen innerhalb beider Subsysteme unterschiedliche Lösungen zur Authentifizierung zum Einsatz. Das hat sowohl historische als auch technische Gründe: Smart-Cards wurden bereits seit einiger Zeit im hochsicheren Ops-Netz genutzt, das auf Linux-Server und -Clients aufbaut. Die dort implementierte Software zur Benutzerauthentifizierung wäre nach Einschätzung Feins und Stößners nur mit größter Mühe in die Windows-Domain zu übertragen gewesen. Zudem ist das bereits eingeführte Smart-Card-System der Linux-Infrastruktur nicht kompatibel zur Windows-Welt. Es war also technisch nicht mit vertretbarem Aufwand möglich, dieses direkt auf die anderen Subsysteme auszuweiten. Mittels der Comtarsia-Lösung als Authentifizierungsschnittstelle zwischen den beiden Systemwelten konnte auch diese Hürde gemeistert werden.

Die Einführung der Lösung ging nach dem Umsetzen aller notwendigen Änderungen problemlos von statten, der produktive Betrieb startete im Juni 2008. Die Anmeldung am PC im Ops-Support-Subsystem erfolgt nun in mehreren Schritten: Zunächst wird anhand der auf der Smart-Card gespeicherten Daten und dem PIN des Users ein Client-Zertifikat erstellt und der Benutzer damit gegen den zentralen LDAP-Server authentifiziert. Ist die Anmeldung am LDAP erfolgreich, wird ein Sign-On-Request an den „SingOn Gate“-Service von Comtarsia abgesetzt, der direkt am Windows-Domain-Controller installiert ist. Dieser Vorgang startet die automatische Benutzerverwaltung im Active Directory: Der Benutzer wird an der Windows-Domäne angemeldet; ist der User dort noch nicht vorhanden, legt das System ihn mit den aus LDAP übernommenen Attributen neu an. Bei jeder Anmeldung sorgt das SignOn-Gate für ein Update der Benutzerinformationen, zum Beispiel

der Gruppenmitgliedschaften, um die im führenden LDAP hinterlegten Daten mit denen des Active Directory zu synchronisieren. Um zu verhindern, dass die Anmeldung am Windows-Arbeitsplatz über Smart-Card und PIN ausgehebelt wird, kommen im Hintergrund zufällig erzeugte Passwörter zur Windows-Anmeldung zum Einsatz.

Fein und Stößner sind mit dem bislang erreichten sehr zufrieden. „Das gesamt Projekt verlief ohne nennenswerte Zwischenfälle“, so Fein. „Alle individuellen Änderungswünsche wurde schnell umgesetzt, wir würden das Projekt jederzeit wieder genau gleich umsetzen.“ Der Return on Investment (RoI) spielte dabei laut Fein keine Rolle. „Es gab unseres Wissens nach keine Alternative, um die Anforderungen der ESA mit der bestehenden Infrastruktur zu erfüllen“, so Fein. Positiv aus Sicht des DLR ist zudem, dass die notwendigen Funktionserweiterungen von Comtarsia in künftige Versionen der Sign-On-Lösung integriert werden. Somit bleibt die Implementierung des DLR Release-fähig, Updates oder neue Versionen können ohne aufwändige Anpassungen eingespielt werden.

((TEXTKASTEN))

Columbus

Columbus ist ein Labor-Modul der internationalen Raumstation ISS und wird von der europäischen Weltraumbehörde ESA betrieben. Angedockt wurde Columbus im Februar 2008, nachdem es vom Space Shuttle Atlantis zur ISS transportiert wurde. An Bord des Columbus-Moduls werden verschiedene Experimente durchgeführt, unter anderem im Bereich Materialforschung oder zur Erforschung der Sonne. Die Steuerung des Moduls obliegt dem Deutschen Zentrum für Luft- und Raumfahrt in Oberpfaffenhofen. Bei der Steuerung müssen an die IT höchste Sicherheits- und Verfügbarkeitsanforderungen gestellt werden: Das Columbus-Modul kann im schlimmsten Fall 24 Stunden autark funktionieren. Sollte die Flight Control in Oberpfaffenhofen trotz

hoher Redundanzen bei den Systemen und bei den Kontrollräumen ausfallen, können Kontrollzentren in den USA und in Russland die wichtigsten Funktionen von Columbus steuern. Bei langen Ausfällen oder gravierenden Störungen müsste das Modul evakuiert werden und die Besatzung sich in andere Bereiche der ISS zurückziehen.

((TEXTKASTEN))

Projektsteckbrief

Projektname: Deutsches Zentrum für Luft- und Raumfahrt
Branche: Luft- und Raumfahrt
Projektkategorie: Benutzerauthentifizierung
Kernprodukte: Comtarsia SignOn Gate, Comtarsia Logon Client
Systemumgebung: Windows, Linux, LDAP
Aufwand (Kosten, Personal): k.a.
Herausforderungen: Integration von bestehender Windows-Domain und Active Directory in führendes LDAP. Einführung von Smart-Card-Authentifizierung (PKI) in bestehende Infrastruktur.
Ergebnis: erfolgreich eingeführt
Stand des Projekts/Zeitrahmen: Laufzeit 1,5 Jahre, produktiv seit Juni 2008
Involvierte Anbieter/Dienstleister: INSYEN AG, Comtarsia IT Services GmbH
Ansprechpartner: Harald Stößner (INSYEN)
Jürgen Fein (DLR)