Sicherheit im Remote-Service und -Support für intelligente Geräte

Sicherheit steht sowohl für Leica Microsystems als auch für die Kunden von Leica Microsystems, die unser Remote-Serviceangebot nutzen, an oberster Stelle. Aus diesem Grund muss die für den Remote-Service verwendete Lösung Schutz gegen Viren und Hacker bieten und unsere intelligenten Geräte ohne aufwändige Anpassungen durch den Endbenutzer unterstützen; gleichzeitig muss sich diese Lösung nahtlos in unser aktuelles Modell für die Netzwerksicherheit einfügen und über ein offiziell anerkanntes Sicherheitszertifikat verfügen. Da die Geräte von Leica Microsystems mit den Kundennetzwerken verbunden werden, fordern die Endkunden mit gutem Recht, dass diese Lösung für den Remote-Service ihr Sicherheitsmodell unterstützt, eine gezielte Steuerung der Zugriffsberechtigungen ermöglicht und eine anwenderfreundliche Möglichkeit der Auditierung und Rückverfolgung bietet.

Im Rahmen des neuen Remote-Serviceangebots RemoteCare erbringt Leica Microsystems, wie zahlreiche andere Gerätehersteller, einen Remote-Service, der die wichtigsten Ressourcen eines Unternehmens schützt; dabei kommen die von Axeda® entwickelte Software ServiceLink™ sowie eine Server-Infrastruktur zum Einsatz. Axeda ServiceLink ist auf die Sicherheitsanforderungen von Leica und Leica-Kunden zugeschnitten und minimiert durch gezielte Maßnahmen eventuelle Ausfallzeiten. Auf diese Weise wird das potenzielle Risiko aktiv reduziert und eine maximale Leistungsfähigkeit der verwendeten Geräte sichergestellt.

Mit Hilfe von Axeda ServiceLink ist RemoteCare von Leica Microsystems in der Lage, eine direkte Verbindung von Leica Microsystems zu den Leica Microsystems-Geräten an den Kundenstandorten herzustellen. Da diese Geräte oftmals zur Aufzeichnung von Patientendaten und anderer persönlicher, geschützter Informationen eingesetzt werden, gehören die Sicherheits- und Datenschutzfunktionen zu den wichtigsten Anforderungen, die eine Fern-Servicelösung erfüllen muss. In dem vorliegenden Dokument werden die Anforderungen von Leica Microsystems und Leica Microsystems-Kunden untersucht. Basierend auf dieser Anforderungsanalyse wird dargestellt, wie mit Hilfe von Axeda ServiceLink ein zuverlässiger und sicherer Remote-Service und -Support erbracht werden kann, der diese Anforderungen erfüllt.

Sicherheit von Remote-Servicelösungen: Die Anforderungen aus Sicht von Leica Microsystems

Leica Microsystems hat sich bei der Umsetzung von RemoteCare für Axeda-Produkte entschieden, um für die Kunden von Leica Microsystems die strengsten Sicherheitsanforderungen zu erfüllen. Damit können Kunden den Remote-Service effektiv und regelmäßig einsetzen – mit dem beruhigenden Wissen, dass die genutzten Datenverbindungen sicher und geschützt sind.
Zu den wichtigsten Anforderungen zählen:

- Unternehmensweit bewährte Struktur: Wann immer ein Computer an das Internet angeschlossen wird, steht die Sicherheitsfrage im Raum. Intelligente Geräte bilden dabei keine Ausnahme. Ob nun Hacker versuchen, ein Gerät mit manipulierten Daten oder einem Virus zu infizieren, Daten auf dem Übertragungsweg zwischen dem Gerät und Leica Microsystems abzufangen oder unberechtigterweise auf kritische Informationen zuzugreifen - ein Remote-Überwachungssystem muss einen wirksamen Schutz vor diesen und anderen Formen der Bedrohung bieten.

- Unterstützung unterschiedlicher Gerätetypen: Leica Microsystems muss einen sicheren Support für unterschiedliche Gerätetypen und komplexe Kundenkonfigurationen ohne aufwändige Anpassungen durch den Endbenutzer bieten.

- Schnelle Einsatzfähigkeit: Kunden können nur dann Remote-Servicelösungen einsetzen, wenn ihr aktuelles Modell für die Netzwerksicherheit die entsprechende Sicherheitsfunktionen enthält.

- Validierung durch externe Sicherheitsunternehmen: Eine offizielle Zertifizierung im Rahmen einer Sicherheitsüberprüfung untermauert das Vertrauen der Kunden in die Fähigkeiten der Technologie und des Lieferanten.

Leistungszusage:
Leica Microsystems weiß, dass Datenschutz und Sicherheit aus Kundensicht höchste Priorität haben. RemoteCare erfüllt die folgenden Sicherheitsanforderungen:

- Schutz der Unversehrtheit des gesamten Systems – Netzwerk, Geräte und Daten
- Aufzeichnung von Benutzerzugriffen und -aktivitäten entsprechend der gesetzlichen Anforderungen
- Flexibilität und Steuerung bei der Umsetzung von Unternehmensrichtlinien
- Auditierung und Zertifizierung der Prozesse und Lösungen von Leica Microsystems in regelmäßigen Intervallen durch eine externe Stelle

Sicherheit von Remote-Servicelösungen: Die Anforderungen aus Sicht der Kunden
Intelligente Geräte werden an die Netzwerke unserer Kunden angeschlossen. Dabei verfügt jeder Kunde über eine eigene Sicherheitsrichtlinie, durch die das Netzwerk in Form von Firewalls, Proxy-Servern und Adressierungsplänen geschützt werden soll. Auch Geräte, die an derartige Kundennetzwerke angeschlossen werden, sind durch diese Sicherheitsvorkehrungen geschützt. Sollte ein Remote-Serviceangebot Änderungen am Netzwerkschutz eines Kunden erfordern, wäre dieses Anliegen vermutlich zum Scheitern verurteilt. Aus diesem Grund ist es wichtig, die Anforderungen der Kunden zu berücksichtigen. Hierzu gehören:

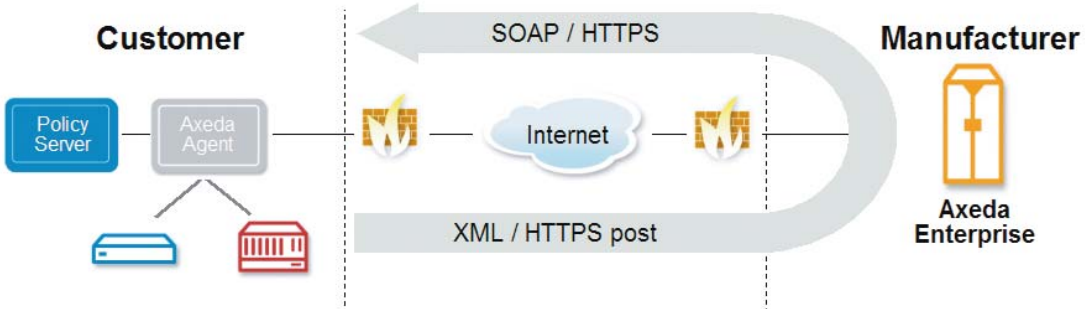
- Beibehaltung des aktuellen Sicherheitsmodells: Die eingesetzten Leica Microsystems-Geräte müssen die etablierte Vorgehensweise der Organisation im Umgang mit sicherheitsrelevanten Vorgängen, Sicherheitsrichtlinien und Sicherheitsverfahren unterstützen und sollten auf anerkannten Industriestandards basieren.

- Steuerung von Benutzerzugriffen: Basierend auf dem Sicherheitsmodell des Kunden müssen Leica Microsystems-Geräte dem Kunden – nicht Leica Microsystems – eine gezielte Steuerung der Benutzerberechtigungen ermöglichen. So kann ein Kunde festlegen, welche Aktionen zu welchem Zeitpunkt auf dem Gerät ausgeführt werden können, z. B. Erfassung von Daten oder Ausführung von Software-Updates. Diese Festlegungen müssen an zentraler Stelle für alle Geräte an einem Kundenstandort getroffen werden.

- Auditierung und Rückverfolgung: Auf Grund interner und gesetzlicher Vorgaben müssen die in Unternehmen eingesetzten Systeme eine Auditierung und Rückverfolgung aller Benutzeraktivitäten bei geringem administrativem Aufwand ermöglichen.

Basierend auf einer Vielzahl an Datenschutzvorkehrungen und Sicherheitsfunktionen bietet Axeda ServiceLink die Leistungsfähigkeit, Flexibilität und Skalierbarkeit, die erforderlich sind, um die Anforderungen der RemoteCare-Kunden von Leica Microsystems auf breiter Basis zu erfüllen.

Abbildung 1: Verbindungen mit Axeda Firewall-Friendly™



Keine Änderung an der IT- oder Sicherheitsinfrastruktur erforderlich
Mit Hilfe der Firewall-Friendly™ Technologie von Axeda ermöglicht RemoteCare eine Zweiwege-Kommunikation auf der Grundlage allgemeiner Standards für internetgestützte Dienste, z. B. HTTP (Hypertext Transfer Protocol), SOAP (Simple Object Access Protocol) und XML (eXtensible Markup Language). Zur Realisierung der Remote-Überwachung und -diagnose müssen keinerlei Änderungen an der IT-Sicherheitsinfrastruktur des Endkunden vorgenommen werden. Daneben werden alle Datenübertragungen zwischen dem Rechenzentrum von Leica oder einem externen Dienstleister und dem Kundenstandort mit Hilfe des SSL-Protokolls (Secure Sockets Layer) mit bis zu 168 Bits verschlüsselt.

Kein VPN und kein Modem erforderlich
Der RemoteCare-Agent leitet die Kommunikationsverbindung am Gerätestandort innerhalb der sicheren Rechenumgebung ein. Für die Nutzung von RemoteCare muss kein teures VPN eingerichtet werden; auch auf sicherheitskritische Wählverbindungen kann verzichtet werden. Die einzige erforderliche Voraussetzung ist ein Internet-Anschluss.

Die wichtigsten Schutzfunktionen von RemoteCare:
- Firewall-Friendly™ Kommunikationstechnik
- Keine Änderungen an der IT- und der Sicherheitsinfrastruktur erforderlich
- Kein VPN und kein Modem erforderlich
- Konsequente Umsetzung von Unternehmensrichtlinien durch Steuerung sämtlicher Einstellungen durch den Endbenutzer
- Einfache Realisierung und Verwaltung der Benutzer-, Anwendungs- und Gerätesicherheit
- HTTPS, PKI und 128-Bit-SSL-Verschlüsselung von Daten

Einfache Steuerung der Benutzerauthentifizierung und der Zugriffsberechtigungen
Das RemoteCare-System verwendet den LDAP-Standard (Lightweight Directory Access Protocol) zur Authentifizierung von Benutzern.

Die Steuerung des Benutzerzugriffs erfolgt über Zugriffsberechtigungen für einzelne Aktionen und Geräte. Diese Zugriffsberechtigungen lassen sich gezielt kombinieren, damit alle Benutzer ihre jeweiligen Aufgaben wirksam erledigen können und der Zugang zu vertraulichen Informationen jederzeit geschützt ist.

Über die aktionsbasierte Zugriffssteuerung kann der RemoteCare-Systemadministrator Benutzer über den Axeda ServiceLink benennen und zu Gruppen zusammenfassen und diesen Benutzern oder Benutzergruppen Berechtigungen für bestimmte Aktivitäten zuweisen. Dadurch verfügt jede Benutzergruppe über einen klar definierten Zugriff auf die Axeda-Anwendungen bzw. einzelne Seiten und Funktionen.

Über die gerätebasierte Zugriffssteuerung können bestimmte Geräte festgelegt werden, auf die die einzelnen Benutzergruppen Zugriff haben. Bei dieser Methode sind für einzelne Benutzer oder Benutzergruppen nur diejenigen Geräte überhaupt sichtbar, für die der Benutzer oder die Benutzergruppe verantwortlich ist.

Sichere Kommunikation und Schutz der Vertraulichkeit der Daten
Ein Großteil der Informationen, die im öffentlichen Internet ausgetauscht werden, besteht aus einfachem Text, der in Standard-HTTP-Nachrichten eingebunden ist. Hacker können sich in der Nähe des Ausgangs- oder des Zielpunkts einer Nachricht Zugang zum Netzwerk verschaffen und den Text dieser HTTP-Nachrichten mit allgemein verfügbaren Tools abfangen und lesen.

RemoteCare unterstützt über die Axeda-Software und -Serverinfrastruktur dieselbe Standard-SSL-Verschlüsselung, die auch von Banken für Online-Geschäfte eingesetzt wird. SSL unterstützt eine Schlüssellänge von bis zu 168 Bit sowie die gegenseitige Authentifizierung über Zertifikate. Daneben ist RemoteCare in der Lage, die AES-Nachrichtenverschlüsselung mit 256 Bit und einem geheimen Schlüssel zu aktivieren, die für die SSL-Verschlüsselung von Daten auch außerhalb der DMZ (entmilitarisierte Zone) eingesetzt werden kann.

Bewährt im Einsatz auf der ganzen Welt
RemoteCare wird auf der ganzen Welt von Herstellern in den verschiedensten Branchen eingesetzt, z. B. im Heimatschutz in den USA, in der Medizintechnik und den Life Sciences, in der Informationstechnik und der Telekommunikation, in der Druckindustrie, bei der Bildgebung, an Informationskiosks sowie in der Halbleiterindustrie und der Industrie- und Gebäudeautomatisierung.

Sicherheitsmerkmale und Vorteile

Basierend auf der Axeda-Technologie bietet RemoteCare die folgenden Sicherheitsmerkmale und Vorteile

Netzwerksicherheit

Merkmale:
- Die Firewall-Friendly™ Technologie basiert auf allgemeinen Standards für internetgestützte Dienste, z. B. HTTP, SOAP und XML.
- Der Verbindungsaufbau geht immer vom Axeda-Agent aus, so dass Geräte keine öffentliche IP-Adresse benötigen und außerhalb der Firewall nicht sichtbar sind.

Vorteile:
- Die Kunden müssen keine Änderungen an den Firewall-Einstellungen oder Proxy-Servern vornehmen. Das vereinfacht die Umsetzung des Konzepts sowie die Einhaltung interner und rechtlicher Vorgaben.
- Für den Einsatz des Systems ist weder ein VPN noch eine Modemverbindung erforderlich.

System- und Datenschutz

Merkmale:
- Die SSL-Verschlüsselung unterstützt eine Schlüssellänge von bis zu 168 Bit sowie die gegenseitige Authentifizierung über bidirektionale digitale Zertifikate.
- Möglichkeit der AES-Nachrichtenverschlüsselung mit 256 Bit und Geheimschlüssel zur SSL-Verschlüsselung von Daten außerhalb der DMZ.

Vorteile:
- Der Zugriff auf einzelne Geräte und Daten ist nur mit der jeweiligen Berechtigung möglich. So kann ein Endkunde seinen Benutzern gezielt Zugriffsrechte, z. B. zur Ansicht von Daten und/oder zur Ausführung von Aktionen, entsprechend des jeweiligen Aufgabengebiets der einzelnen Benutzer zuordnen.
- Eine bewährte, auf allgemeinen Standards basierte Kommunikationstechnik stellt die Einhaltung der gesetzlichen Anforderungen sicher.

Benutzer- und Anwendungsschutz

Merkmale:
- Der Zugriff auf das System wird zentral gesteuert und mit Hilfe eines unternehmensweiten LDAP-Systems authentifiziert.
- Obligatorische Verwendung starker Passwörter – bestehend aus mindestens sechs Zeichen, die eine Kombination aus Buchstaben, Zahlen und Symbolen darstellen.
- Sämtliche über einen dezentralen Zugang ausgeführten Aktionen werden durch das System verfolgt und aufgezeichnet.

Vorteile:
- Die Kunden können bereits bestehende LDAP-Benutzerkonten nutzen und haben somit keinerlei Anlaufschwierigkeiten.
- Den Endbenutzern steht ein umfassendes Auditierungsprotokoll zur Verfügung, mit dessen Hilfe auch die Aktivitäten von Lieferanten im Hinblick auf die Einhaltung der gesetzlichen Bestimmungen analysiert werden können.

Zusammenfassung
Leica Microsystems hat sich bei seinem RemoteCare-Angebot für Axeda ServiceLink entschieden, um ein Maximum an Sicherheit zu gewährleisten. Unternehmen auf der ganzen Welt setzen Axeda ServiceLink ein, um ihren Kunden einen sicheren Remote-Service anbieten zu können. Diese weltweite Akzeptanz liegt darin begründet, dass Axeda bei der Entwicklung der Axeda-Infrastruktur und der Axeda-Dienste die allgemein anerkannten Sicherheitsgrundsätze und -normen sorgfältig berücksichtigt. Wie bei Leica Microsystems genießt die maximale Sicherheit auch bei Axeda höchste Priorität - damit die Kunden ihre jeweiligen Ziele für den Fern-Service sicher und effizient realisieren können.