PKI mit Hardware-Sicherheitsmodul

Landschaftsverband Rheinland: sicherer und bürgernaher IT-Service

IT-Sicherheit. Der Betrieb von 120 Webservern und rund 8.000 PCs sowie die Anbindung von mehreren hundert Heimarbeitern stellen den Landschaftsverband Rheinland (LVR) vor große Herausforderungen an die IT-Sicherheit. Der Kommunalverband der rheinischen Städte und Kreise schützt seine gesamten IT- und Web-Anwendungen deshalb mit einer neuen Public-Key-Infrastruktur (PKI) in Verbindung mit dem Hardware-Sicherheitsmodul (HSM) SafeGuard CryptoServer von Utimaco.

OLIVER HOFFMANN ist Geschäftsführer von LVR InfoKom, dem IT-Dienstleister des LVR

Der Landschaftsverband Rheinland (LVR) arbeitet mit rund 15.000 Beschäftigten für 9,6 Millionen Menschen in den 14 kreisfreien Städten und 13 Landkreisen im Gebiet Nordrhein. Als Betreiber von 40 Förderschulen, zehn Kliniken und einem heilpädagogischen Netzwerk ist der LVR zudem größter Leistungsträger für Menschen mit Behinderungen in Deutschland. Neben den Aufgaben in der Behinderten- und Jugendhilfe sowie in der Psychiatrie hat der LVR aber auch noch einen kulturellen Auftrag als Träger von sechs Museen zu erfüllen.

Eine Institution dieser Größenordnung, die aus verschiedenen dezentralen Einrichtungen besteht, setzt natürlich die unterschiedlichsten IT-Systeme ein: Dazu gehören zahlreiche Thin Clients, PCs, Workstations und 120 Webserver der verschiedensten Technologie-Plattformen wie IIS, Tomcat, Apache, SAP und Lotus Notes Domino, die das IT-Systemhaus InfoKom – eine hundertprozentige LVR-Tochter – in zwei ausfallsicheren Hochsicherheitsrechenzentren in Köln zentral betreibt. Für alle LVR-Mitarbeiter sind folgende Anwendungen über ein Datennetz oder über das Internet permanent erreichbar und verfügbar:

- Zentrale Software für rund 8.000 PCs, Workstations und Clients,
- Outlook WebAccess (OWA) für mehrere hundert Mitarbeiter, die täglich auf Dienstreisen oder von zu Hause aus ihre Mails abrufen.

Darüber hinaus sind rund 800 Home-Office-Anwender permanent an den LVR angebunden. Und auch den Kunden von LVR-InfoKom werden zusätzlich unterschiedliche Anwendungen zur Verfügung gestellt wie beispielsweise:

- „Klifd“ („Klientenverwaltungsprogramm für Integrationsfachdienste“) – ein eigenständiges Bearbeitungs- und Dokumentationsprogramm für die Arbeit mit beschäftigten und arbeitslosen behinderten Menschen;
- „KulaDig“ („KulturLandschaft Digital“) – Nordrhein-Westfalens webbasierendes Informationssystem über die Kulturlandschaften (unter anderem mit historisch-geografischen, boden- und baudenkmalpflegerischen Fachdaten);
- spezielle SAP-Anwendungen (beispielsweise für die Gehaltsabrechnungen);
- Webseiten von Schulen und Einrichtungen der Jugend- und Sozialhilfe sowie von Kliniken und verschiedenen Kulturdienststellen, die zusätzlich von InfoKom als LVR-Subdomains gehostet werden.

Das LVR-Motto „Qualität für Menschen“ gilt auch für die IT-Sicherheit.

„Der Anspruch an die Arbeit aller LVR-Einrichtungen ist hoch: Jede Leistung, hinter der der LVR steckt, hat eine besonders hohe fachliche und zugleich menschliche Qualität. Das will der LVR mit dem Slogan ‚Qualität für Menschen’ ausdrücken“, erläutert Oliver Hoffmann, Geschäftsführer von LVR InfoKom. Diesen hohen Qualitätsanspruch legt der Landschaftsverband Rheinland auch an seine IT-Sicherheit an. Deshalb betreibt InfoKom schon seit 2002 eine – aus heutiger Sicht – rudimentäre Public-Key-Infrastruktur (PKI) auf Windows-2000-Basis für die SSL-Verschlüsselung verschiedener Web-Applikationen (wie von Online-Datenbankanwendungen). Jedoch reichte das Sicherheitsniveau der alten PKI-Lösung, die einer Windows-Basic-Authentifizierung entsprach, bei Weitem nicht mehr aus. Zudem lief die Gültigkeit des vorhandenen LVR-Rootzertifikates ab, wodurch die Stilllegung aller Webserver drohte.

Deshalb wurde die alte, auslaufende PKI im Oktober 2007 gegen eine neue Public-Key-Infrastruktur abgelöst, die das Systemhaus InfoKom gemeinsam mit Microsoft und dem IT-Sicherheitsspezialisten Utimaco implementierte. Durch qualitativ hochwertigere Schlüsselpaare mit doppelt so langen RSA-Schlüsseln von 2048 Bit bietet das neue Sicherheits-Framework ein deutlich höheres Sicherheitsniveau als die bisherige PKI.

Hardware-Sicherheitsmodul schützt die Signaturschlüssel

Um eine PKI wirksam abzusichern und um die Integrität der Zertifikate zu gewährleisten, muss der CA-Schlüssel (Certification-Authority- oder Signaturschlüssel) jedoch sehr sorgfältig geschützt werden. Diese Schutzfunktion der CA-Schlüssel übernimmt das Hardware-Sicherheitsmodul (HSM) SafeGuard CryptoServer von Utimaco, in dem die CA-Schlüssel sicher erzeugt, gespeichert und gegen unberechtigten Zugriff oder Manipulation geschützt werden. Hardware-Sicherheitsmodule sind eine eigene Geräteklasse, die extra für die sichere Speicherung und Verarbeitung von sensiblen, kryptografischen Objekten und Operationen konzipiert wurden.

Mit dem SafeGuard CryptoServer wird so die Integrität der digitalen Zertifikate und der gesamten PKI aufrecht erhalten – und damit auch die Vertrauenswürdigkeit der kompletten Geschäftsprozesse und Verwaltungsabläufe, die mit der PKI abgesichert werden.

„Der SafeGuard CryptoServer von Utimaco ermöglicht eine absolut manipulationssichere Signaturerstellung und Schlüsselgenerierung und bietet so ein maximales Sicherheitsniveau“, bestätigt Hans-Jörg Kandt, PKI-Projektleiter bei LVR InfoKom. Um eine hohe Interoperabilität zu gewährleisten, basiert die neue PKI – genauso wie die alte Lösung – auf Microsoft-Technologie und ist für die gesamte LVR-Belegschaft ausgelegt. Beim Rollout der PKI wurden schrittweise alle LVR-Server mit neuen SSL-Webserver-Zertifikaten ausgestattet. So wird sichergestellt, dass Informationen, die etwa in verschiedene Formulare auf den entsprechenden Webseiten von Schulen, Sozial- und Jugendhilfe- oder Kultureinrichtungen sowie Kliniken eingegeben und abgeschickt werden, während der Übertragung zwischen einem LVR-Webserver und den Webbrowsern der Anwender verschlüsselt werden.

Jetzt werden alle Notebooks verschlüsselt

Außerdem erhielten rund 8.000 PCs, Workstations und Clients IPSec-Maschinen-Zertifikate, die die Basis für interoperable und sichere Host-to-Host- oder Client-to-Host-Verbindungen bilden. Schließlich wird die PKI noch zur sicheren Teilnehmerauthentifizierung innerhalb der WLAN-Infrastruktur des LVRs eingesetzt. Als künftige PKI-Anwendungen nennt Projektleiter Kandt die geplante Authentifizierung und eMail-Signatur für alle LVR-Mitarbeiter per Smartcard oder Token sowie die Verschlüsselung aller Notebooks der Organisation.

„Trotz eines engen Zeitplans konnten wir die Umstellung der PKI beim LVR durch die gute Zusammenarbeit mit den Projektpartnern Microsoft und Utimaco fristgerecht und erfolgreich umsetzen“, betont Hans-Jörg Kandt, Projektleiter bei LVR InfoKo: „Unsere Kolleginnen und Kollegen profitieren von einem sehr modernen und sicheren System, mit dem sie permanent auf alle wichtigen Daten zugreifen können.“

Detlev Spierling

WORTWEISER 1

PUBLIC-KEY-INFRASTRUKTUR (PKI)

Das Konzept einer Public-Key-Infrastruktur (PKI) basiert auf dem gebräuchlichsten asymmetrischen Verschlüsselungsalgorithmus RSA, der 1977/78 am Massachusetts Institute of Technology (MIT) von Ron Rivest, Adi Shamir und Len Adleman entwickeltet und nach den Initialen ihrer Nachnahmen benannt wurde.

Bei diesem kryptografischen Verfahren verwenden Sender und Empfänger zur Chiffrierung und Dechiffrierung ein Schlüsselpaar, das aus einem öffentlichen Schlüssel (public key) und seinem geheimen Gegenstück (dem private key) besteht. Will ein Sender ‚S’ eine vertrauliche Information an den Empfänger ‚E’ übermitteln, so chiffriert er sie mit dessen öffentlichem Schlüssel. Am anderen Ende dechiffriert der legitime Empfänger – und nur er – die Nachricht mit seinem geheimen Schlüssel. Auf diese Weise ist während des gesamten Vorgangs die Vertraulichkeit gesichert, denn selbst wenn es Datendieben gelingt, eine Nachricht abzufangen, können sie ohne geheimen Schlüssel nicht auf die darin enthaltenen Informationen zugreifen.

Damit das funktioniert, muss der öffentliche Schlüssel allgemein zugänglich sein, der private oder geheime Schlüssel dagegen unbedingt geheim bleiben. Die Vertrauenswürdigkeit des öffentlichen Schlüssels eines PKI-Nutzers wird per digitaler Signatur mit einem Zertifikat dokumentiert.

WORTWEISER 2

SICHERHEITS-FRAMEWORK

Der Begriff PKI bezeichnet den technischen und organisatorischen Rahmen, innerhalb dessen auf asymmetrischer Verschlüsselung basierende Sicherheitsfunktionen bereitgestellt werden.

Neben Protokollen, Diensten und Standards, die eine einheitliche Umsetzung garantieren, bedarf es zu ihrem Aufbau zweier Instanzen, der Zertifizierungsstelle (Certification Authority – CA) und der Registrierungsstelle (Registration Authority – RA), welche die eindeutige Zugehörigkeit eines Schlüsselpaares zu einem User bestätigen (zertifizieren) und so die notwendige Vertrauensbasis schaffen.

Im Einzelnen haben sie folgende Aufgaben:

- Die Registration Authority (RA) nimmt Anträge auf Erteilung eines digitalen Zertifikats entgegen, überprüft die Identität eines jeden Antragstellers (Name, eMail-Adresse, Postanschrift) und leitet den Antrag und das Ergebnis der Prüfung an eine CA weiter.
- Die Certification Authority (CA) ist dazu da, die gewünschte Bescheinigung auszustellen und an den Antragsteller zu übermitteln. Im Rahmen einer PKI gewährleistet sie die Zuordnung öffentlicher Schlüssel zu ihren Inhabern und steht für deren Richtigkeit gerade. Bei der Generierung eines Zertifikats bedient sich die CA vorgegebener Policies (Richtlinien), die etwa die Gültigkeitsdauer oder zusätzliche Einsatzzwecke eines Schlüssels festlegen – beispielsweise wenn dieser außer zur Anmeldung im Netz auch zum Signieren von eMails dienen soll. Nach der Zertifizierung legt die CA den public key in einer frei zugänglichen Datenbank oder auf einem Verzeichnis-Server (Repository) ab. Der private key dagegen darf, wie bei RSA, nur dem Benutzer bekannt sein und sollte aus Sicherheitsgründen auf einer Smartcard oder einem Token gespeichert werden.

PRODUKT-INFO

Das Hardware-Sicherheitsmodul (HSM) SafeGuard CryptoServer von Utimaco bietet den höchstmöglichen Schutz zur Absicherung vertraulicher Geschäftsprozesse. Es sorgt für die sichere Generierung, Speicherung und Verarbeitung von kryptografischen Schlüsseln und Zertifikaten bei Verschlüsselungs- und Signaturverfahren. Die Lösung ist Teil der Produktpakete aus der umfangreichen SafeGuard-Produktfamilie und ist standardmäßig in allen Microsoft-Servern einsetzbar. Dadurch hat der Anwender keinen zusätzlichen Integrationsaufwand. Der SafeGuard CryptoServer wurde zum zweiten Mal in Folge vom amerikanischen National Institute of Standards and Technology (NIST) und dem kanadischen Communications Security Establishment (CSE) nach dem Sicherheitsstandard FIPS (Federal Information Processing Standard) 140-2, Level 3 zertifiziert. Die FIPS-Zertifizierung Hardware-basierender Verschlüsselungsmodule ist in der Industrie und der Privatwirtschaft weltweit als IT-Standard anerkannt.

PROFILE

LVR INFOKOM

Die 1962 gegründete InfoKom ist das IT-Systemhaus für den Landschaftsverband Rheinland (LVR) und versorgt den gesamten Verband sowie weitere Kunden wie Kliniken, Schulen und Kommunen mit modernen IT-Serviceleistungen. Damit der LVR seine Aufgaben bestmöglich erfüllen kann, stellt LVR InfoKom dem Landschaftsverband Rheinland ein leistungsfähiges IT-System zur Verfügung. Zu diesem Zweck betreibt das IT-Systemhaus zwei ausfallsichere Hochsicherheitsrechenzentren in Köln, in denen alle wichtigen Verfahren des LVR realisiert, gepflegt und weiter entwickelt werden.

InfoKom sorgt dafür, dass die zentralen Systeme für alle Mitarbeiterinnen und Mitarbeiter über ein Datennetz permanent erreichbar sind und die erforderliche Software auf den PCs am Arbeitsplatz verfügbar ist. Neben dieser „Versorgung“ unterstützt er seine Kunden bei der Analyse und Optimierung der Geschäftprozesse, die mit IT-Unterstützung wirtschaftlicher und bürgernäher gestaltet werden können.

InfoKom versteht sich als Partner und Berater seiner Kunden, der dazu beiträgt, dass sie ihre Aufgaben effektiv und wirtschaftlich erfüllen können. Zudem verfügt das IT-Systemhaus über ein modernes IT-Schulungszentrum mit jährlich über 2.500 Absolventen und ist ein anerkannter und zertifizierter SAP-Partner. Seit 2005 ist InfoKom ein Eigenbetrieb und wird nach den Grundätzen eines eigenständigen Unternehmens geführt.

UTIMACO SAFEWARE AG

Als Hersteller von Datensicherheitslösungen ermöglicht Utimaco mittelständischen und großen Unternehmen sowie Organisationen ihre elektronischen Werte vor Angriffen zu schützen und deren Vertraulichkeit und Integrität gemäß den geltenden Datenschutzbestimmungen zu wahren.

Als Reaktion auf die Sicherheitsbedrohungen des 21. Jahrhunderts bietet Utimaco eine umfangreiche Lösungspalette für den umfassenden 360-Grad-Schutz von Daten an. SafeGuard-Lösungen von Utimaco unterscheiden sich damit deutlich von Punktlösungen, die nur sehr spezifische Sicherheitsanforderungen erfüllen.