Christoph Wildensee

Auf der Intensivstation – Ausspähen ist eine Frage der Gelegenheit

1 Einleitung

Das "Lightweight Directory Access Protocol" (LDAP) ermöglichst die Zurverfügungstellung von Informationen eines zentralen Verzeichnisdienstes bidirektional als Datenbankabfrage. Dies bedeutet, dass per LDAP Mail-Adressdaten zur Kommunikation und auch andere Stammdaten für eine weitere Verarbeitung in SAP bereitgestellt werden können. Die SAP-Dokumentation stellt fest: "Das Lightweight Directory Access Protocol (LDAP) ist ein Client / Server-Protokoll für den Zugriff auf Adressverzeichnisse (Directories) […]. Dieses Protokoll erlaubt es einem LDAP-Client, der üblicherweise in ein Mail-System integriert ist, Adressdaten wie z. B. Telefonnummern, Namen, Funktionsbeschreibung, Postfach, E-Mail-Adressen, aber auch Rechneradressen, Bilddaten oder RSA-Public-Keys für verschlüsselte Nachrichtenübertragung aus dem Adressverzeichnis zu lesen oder solche Adressdaten in das Adressverzeichnis zu schreiben. […] Der Datenbestand der Adressverzeichnisse ist in der Regel auf mehrere (LDAP-)Server verteilt. Der Client muss über den Aufbewahrungsort der gesuchten Daten keine Information besitzen, da diese Informationen von den Servern […] untereinander ausgetauscht werden."

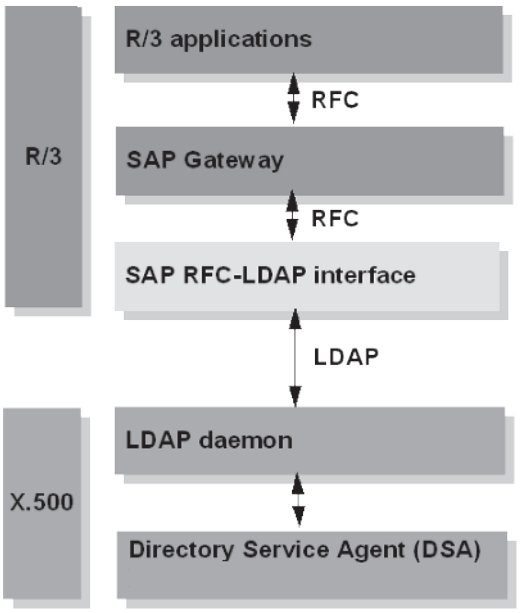

Abb. 1: Beispielkonfiguration einer SAP RFC-LDAP-Schnittstelle (Quelle: SAP).

Die Kommunikation aus SAP heraus erfolgt über einen speziellen RFC-User, der in der definierten Kommunikationsverbindung hinterlegt wird. Ein solcher User kann natürlich, wenn sein Kennwort bekannt ist, ggf. auch für andere Zwecke verwendet werden. Insoweit sind die Kennwörter solcher Schnittstellenuser möglichst restriktiv zu handhaben bzw. nur einem kleinen Kreis an Berechtigten bekanntzugeben.

2 Das Sicherheitsleck

Umso interessanter ist es, wenn SAP die Möglichkeit offeriert, das Kennwort eines eingerichteten Users in Klarschrift anzeigen zu lassen. Der Funktionstest bzw. das Debuggen des Funktionsbausteins "**LDAP_COMMONBIND**" zeigt den unkomplizierten Weg auf. Er liest aus "cred_in" die Zugangsdaten aus, welche dann folgend in dem Funktionsbaustein "**LDAPRFC_BIND**" zur Kommunikationsaufnahme genutzt werden.

Der Aufruf der LDAP-Funktionalität erfolgt über die Transaktion LDAP.

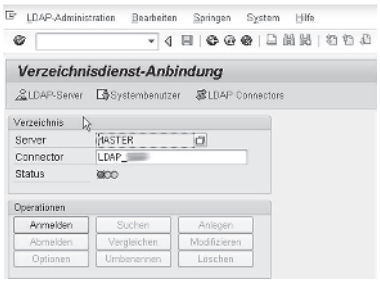

Abb. 2: Aufruf des Verzeichnisdienstes (Transaktion LDAP).

Die Darstellung im Debugging zeigt nicht nur den durchlaufenden Quellcode, sondern auch das mitgegebene Kennwort in Klarschrift in der Variable PWD_STRING.

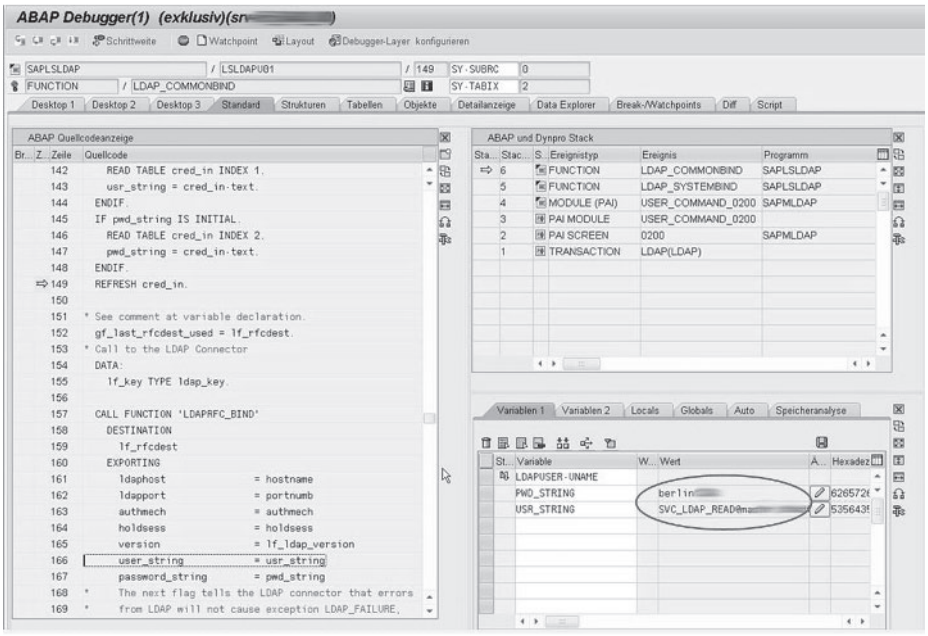

Abb. 3: Aufruf des Debuggers und Identifizierung des PWD_STRING in Klarschrift.

3 Fazit

Es wird nicht die letzte Sicherheitslücke gewesen sein, die sich durch die Integrationsmöglichkeit anderer Systeme und Dienste an ein SAP-System ergibt. Die Kennwortpreisgabe eines Systemusers (an dieser Stelle zum Ausschluss von Kollisionen ggf. sogar der <SID>ADM) ist nachhaltig misslich, denn solche Informationen werden bewusst nur einem begrenztem Kreis der Administratorengruppe bekannt gegeben. Es wird folglich

immer schwieriger, die Frage zu beantworten, wer mit welchen Rechten im Unternehmen auf Informationen zugreifen kann, wenn das Ausspähen von Zugangsdaten so einfach ermöglicht wird. Stark privilegierte Schnittstellen- / Systemuser sind problematisch, denn deren Berechtigungen sind selten an ihrer Aufgabe ausgerichtet, sondern häufig viel weiter gefasst. SAP stellt heraus: "Um die Sicherheit Ihrer Systemlandschaft zu erhöhen, vergeben Sie beim Anlegen der Systembenutzer nur noch stark eingeschränkte, in speziellen Rollen zusammengefasste Berechtigungen an die Systembenutzer" und es sollte (wegen der nicht unerheblichen Mehrarbeit bei Kennwortänderungen eines Systemusers) in der "[…] Systemlandschaft ebenso viele Systembenutzer wie RFC-Destinationen" geben. Dies kann das Problem verringern, ist aber selten in der Praxis vorzufinden. Die Reduzierung der hier grundlegenden Berechtigungen (z. B. Transaktion LDAP [Customizing & Text]; Berechtigungsobjekt S_LDAP) auf zwei oder drei Basisadministratoren und der Ausschluss des Zugriffs und auch des Tests für alle anderen Rollen vermag ein gewisses Maß an Sicherheit zu generieren. Gelegenheit macht Diebe.

Literatur

SAP AG RFC-LDAP-Schnittstelle;
http://help.sap.com/saphelp_40b/helpdata/de/6c/69c777418d11d1896e0000e8322d00/content.htm.

SAP AG Trusted / Trusting zwischen SAP Systemen,
http://help.sap.com/saphelp_nw70/helpdata/de/8b/0010519daef443ab06d38d7ade26f4/content.htm.

SAP AG User Mapping with an LDAP connection;
http://wiki.sdn.sap.com/wiki/display/Duetent/User+Mapping+with+an+LDAP+connection.

SAP AG Systembenutzer und RFC-Destinationen;
http://help.sap.com/saphelp_sm32/helpdata/de/23/cbce3b1bc7fa20e10000000a114084/content.htm.

Tiede, Thomas SAP R/3 – Ordnungsmäßigkeit und Prüfung des SAP-Systems (OPSAP),
2. Auflage, Ottokar-Schreiber-Verlag, Hamburg, 2004.

Virtual Forge Ihr SAP-System in 60 Sekunden geknackt;
http://virtualforge.com/tl_files/Theme/Artikel/SD_aus_SH_SAPuSicherheit_2012_Virtual_Forge_150dpi.pdf.

Virtual Forge Real SAP Backdoors;
http://virtualforge.com/tl_files/Theme/Presentations/20120322_Real_SAP_Backdoors_Wiegenstein.pdf.

Virtual Forge SQL Injection with ABAP;
http://virtualforge.com/tl_files/Theme/Presentations/HITB2011.pdf.

Wildensee, Christoph
Nachvollzugsansätze zum Remote Funktion Call in SAP, in: Zeitschrift Interne Revision (Jg. 46) 06/2011, S. 318–326.

Wildensee, Christoph
Externer Zugriff auf SAP R/3-Systeme über RFC, in: PRev Revisionspraxis II/2006, S. 15-19.

Wildensee, Christoph
Aufruf nicht remotefähiger Funktionsbausteine per remotefähigem "Tunnel-Baustein" in SAP,
in: PRev Revisionspraxis VI/2011, S. 304–309.

Dipl.-Betriebswirt Christoph Wildensee (CISM, CRISC) ist seit 1993 als IV-Revisor bei der Stadtwerke Hannover AG tätig. Zusätzlich war er von 02/2008 bis 12/2012 auch Datenschutzbeauftragter. Er ist als Prüfer speziell im SAP-Umfeld über seine zahlreichen Fachveröffentlichungen im deutschsprachigen Raum bekannt.