WERTH

WERTH auditor
sicherheit für sap-systeme

Erkennung und Abwehr

von Sicherheitsrisiken in SAP-ERP Systemen

Inhaltsverzeichnis

Allianz für Cybersicherheit

“Die Allianz für Cyber-Sicherheit ist eine Initiative des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die im Jahr 2012 in Zusammenarbeit mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) gegründet wurde.

Ziele und Angebote der Allianz

Als Zusammenschluss aller wichtigen Akteure im Bereich der Cyber-Sicherheit in Deutschland hat die Allianz das Ziel, die Cyber-Sicherheit in Deutschland zu erhöhen und die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyber-Angriffen zu stärken. Zur gemeinsamen Förderung der Cyber-Sicherheit arbeitet das BSI dabei im Rahmen der Allianz intensiv mit Partnern und Multiplikatoren zusammen.
Zur Erreichung dieser Ziele verfolgt die Allianz die folgenden Maßnahmen:

- Erstellung und Pflege eines aktuellen Lagebilds
- Bereitstellung von Hintergrundinformationen und Lösungshinweisen
- Intensivierung des Erfahrungsaustausches zum Thema Cyber-Sicherheit
- Ausbau von IT-Sicherheitskompetenz in Organisationen mit intensivem IT-Einsatz

Die Allianz für Cyber-Sicherheit baut hierfür eine umfangreiche Wissensbasis auf und initiiert und betreibt Erfahrungs- und Expertenkreise zur Cyber-Sicherheit. Ergänzt werden diese Angebote durch weitere Beiträge der Partner z.B. in Form von Schulungen, zusätzlichen Informationsveranstaltungen oder der kostenlosen Bereitstellung von Sicherheitsprodukten.”
(Quelle: ACS-Homepage https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Ueber_uns/Einfuehrung/einfuehrung.html)

Als Partner der Allianz für Cyber-Sicherheit veröffentlich die Werth IT dieses Dokument.

Einleitung

SAP ist einer der größten Softwarehersteller weltweit. Der Fokus liegt dabei auf Enterprise Resource Planning (ERP) Produkten. In diesen Systemen speichern Unternehmen ihr wahres Kapital – nämlich Ihre Daten.
Die folgenden fünf Anwendungen stellen die wichtigsten Bereiche in SAP dar:

- SAP ERP Central Component (SAP ECC), ehemals bekannt als R/3
- Customer Relationship Management (CRM)
- Product Lifecycle Management (PLM)
- Supply Chain Management (SCM)
- Supplier Relationship Management (SRM)

Zur sicheren Verwahrung der Daten muss das ERP-System über ein hohes Sicherheitslevel verfügen. Gilt es doch Hacker-Angriffe abzuwehren, Wirtschaftsspionage und Datenmanipulation zu unterbinden. Doch wie soll die Sicherheit des Systems bewertet werden, wenn man die Risiken nicht kennt? Zur Sensibilisierung der Risiken von SAP Systemen erfolgt eine bildliche Veranschaulichung der größten Angriffsflächen.

Risiken in SAP Systemen

Risiko kritische Berechtigungen

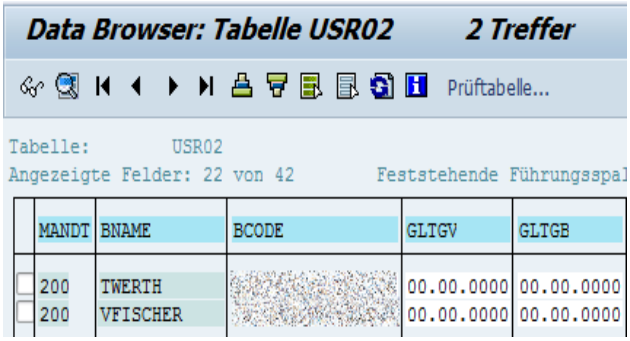
Die bekannteste Absicherung von SAP-Systemen ist dessen Berechtigungskonzept. Leider werden immer noch - teils aus Unwissenheit - kritische Berechtigungen in Produktivsystem vergeben. Ein Beispiel hierzu sind die Berechtigungen “Debuggen mit Wertänderung” oder “alle Tabellen pflegen” zu dürfen. Warum dies kritisch ist soll ein kleines Szenario verdeutlichen:

In dem fiktiven Szenario besitzt der User VFISCHER eben diese Berechtigungen. Wie sich zeigen wird, ist er damit in der Lage die Passwörter aller anderen Benutzer zu ändern.

Der Weg dorthin führt über die Transaktion SE16 und der Anzeige der Tabelle USR02. Diese Tabelle beinhaltet die kernelseitigen Anmeldedaten aller Benutzer.

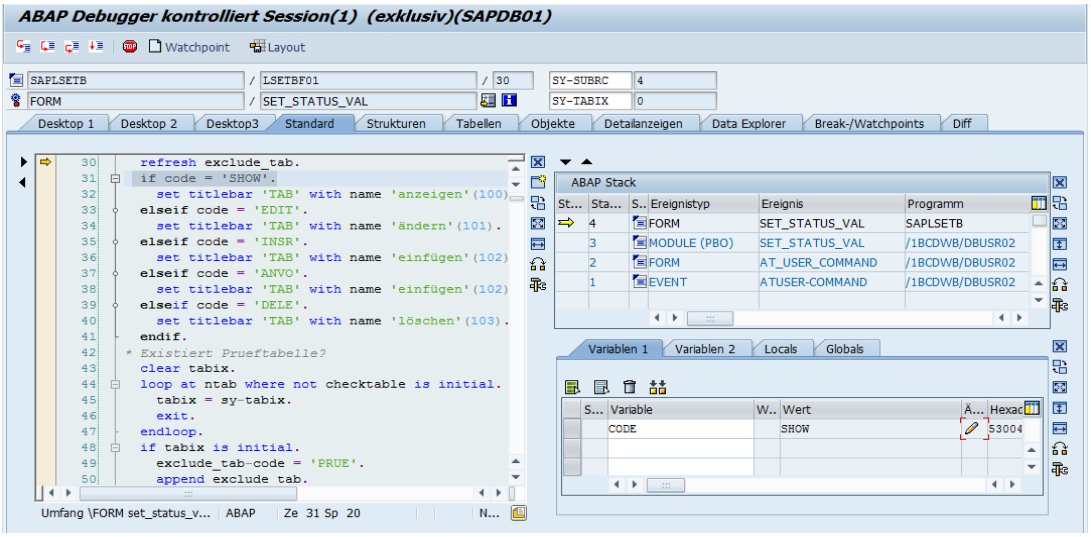
Im Folgenden wird gezeigt, wie er das Passwort des Benutzers TWERTH mit seinem eigenen ersetzen kann.

Dazu selektiert er zunächst beide Benutzer in der Ansicht und klickt anschließend doppelt auf seinen eigenen Eintrag.

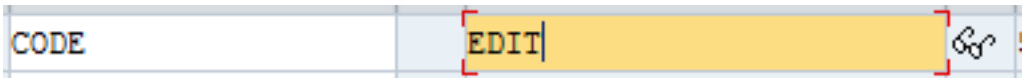


In der neuen Ansicht führt er sodann in der oberen Zeile den Befehl "/h" aus, um das Debugging zu aktivieren und kopiert die Werte aus dem BCODE und PASSCODE Feldern in eine Textdatei.

Anschließend folgt ein Klick auf nächster Eintrag. Es öffnet sich nun die Debugger Ansicht. Zunächst klickt man auf den Standard-Reiter, um die Anzeige zu optimieren.

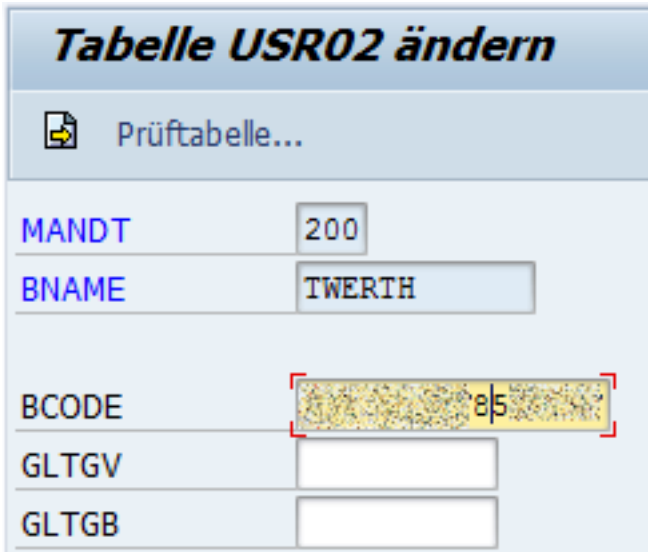


Hier steht man vor der Zeile if code = 'SHOW'." . Durch einen Doppelklick of "code" wird die Variable im Debugger mit Wert angezeigt. Hier klickt man nun auf den Stift und überschreibt den Wert SHOW mit dem Wert EDIT.



Die Ausführung des Programms wird mit F8 fortgesetzt.

Das Editieren der Tabelle USR02 mit den kernelseitigen Anmeldedaten ist nun problemlos möglich und es ist für den Angreifer ein leichtes den eigenen Hashcode aus der Textdatei auch für andere Nutzer zu hinterlegen.



Dieses Beispiel veranschaulicht sehr deutlich wie die Berechtigung zum Debuggen mit Wertänderung vorhandene Sicherheitsmechanismen im SAP-System ausgehebelt haben und somit System-Operationen erlaubten, die diesem User eigentlich untersagt wären. Ein analoges Vorgehen in der Buchhaltung, beispielsweise die Änderung von Kontodaten bei den Kreditoren, hätte direkte finanzielle Auswirkungen zur Folge. Es ist daher immens wichtig die Vergabe von kritischen Berechtigungen regelmäßig zu auditieren.

Risiko Standardzugangsdaten

Im Rahmen einer SAP Installation werden bekannte Standard Zugangsdaten eingerichtet. Diese sind Allgemein bekannt und lassen sich im Internet finden. Eine Änderung diese Daten ist für die Systemsicherheit unumgänglich. Ein Auszug der bekanntesten Zugangsdaten sind:

- SAP*, der Super User mit dem Passwort 06071992 oder PASS.
- DDIC, der ABAP Dictionary Super User mit dem Passwort 19920706
- TMSADM, der Transport Management Super User mit dem Passwort PASSWORD
- EARLYWATCH, der Service User der SAP mit dem Passwort SUPPORT
- SAPCPIC, der Kommunikations User mit dem Passwort ADMIN

Risiko RFC-Schnittstelle

Für Angriffe auf SAP Systeme eignet sich die RFC-Schnittstelle besonders gut. Dies liegt vor Allem an dem schier unendlichen Fundus an Remote-RFC-Funktionsbausteinen, die eine Vielzahl an Zugriffen auf das System bieten. Beispielsweise können mit der Funktion RFC_READ_TABLE ganze SAP Tabellen ausgelesen werden. Diese Funktion hat sicherlich ihren produktiven Nutzen, jedoch kann sie auch für Datendiebstahl verwendet werden. Jüngst entdeckte Trojaner versuchen bereits entsprechende Zugangsdaten abzufangen.

Damit ein Angreifer überhaupt auf RFC zugreifen kann, muss dieser Zugriff auf den Dienst des Systems erhalten. In der Regel ist der RFC Dienst (Port 33XX) nicht aus dem Internet erreichbar. Aber nicht ausreichend konfigurierte SAP Router können hier den Weg aus dem Internet ermöglichen. Alternativ besteht die Möglichkeit RFC über SOAP aus dem Internet ansprechen zu können. Dies sind bereits zwei Wege für externe Angreifer Zugriff auf den RFC Dienst zu bekommen. Doch wenn man bei der NSA Berichterstattung mitliest, wird man zwischen den Zeilen bestätigt, dass ein externer Angreifer sich eh erst Zugang zu dem internen Netzwerk verschafft und dann die dort gelagerten Systeme attackiert.

Zugriff auf den RFC Dienst ist jedoch nicht gleichbedeutend mit dem Zugriff auf die dort angebotenen Funktionsbausteine. Hier greift zunächst das Berechtigungskonzept von SAP. Was allerdings in Bezug auf RFC sehr verzwickt zu konfigurieren ist, will man nach dem Prinzip "so viel wie nötig, so wenig wie möglich" verfahren. Und genau dies kommt Angreifern gelegen. So wird häufig S_RFC * bei den Berechtigungen vergeben, um sich bei RFC nicht zu verzetteln und möglichst keine Drittanbieter Programme auszusperren.

Dies machen sich die Angreifer zu nutze. Entweder konnten Zugangsdaten im Netzwerk abgefangen werden oder Default Accounts wurden nicht geändert. Schon ist der Weg frei für den RFC Zugriff.

Besonders gefährlich wird es wenn nicht regelmäßig die neuesten SAP Hinweise eingespielt

werden. Dies kann diverse Gründe haben, aber faktisch verbleiben so verwundbare Funktionsbausteine im System. Wie der Hinweis 1861791 - Betriebssystembefehl-Injection-Schwachstelle in ST-PI zeigt, können so selbst eher harmlosere Funktionen missbraucht werden, um ein System unter seine Kontrolle zu bekommen.

Ein weiterer Angriffsvektor sind die Registrierten RFC-Server. Diese erlauben teilweise vollen Systemzugriff ganz ohne Anmeldedaten. SAP hat dieses Problem ebenfalls erkannt. Jedoch scheint die Lösung des Problems nicht unproblematisch, daher hat sich SAP entschlossen den Zugriff auf die RFC-Server aus den neuen Versionen der RFC-SDKs zu entfernen, um den Angriffsvektor zu schließen. Fragt sich nur ob die Angreifer auch immer die neuesten SDK Versionen nutzen wollen ...

Sicher ist hier nur, wer die Gateway ACL korrekt konfiguriert.

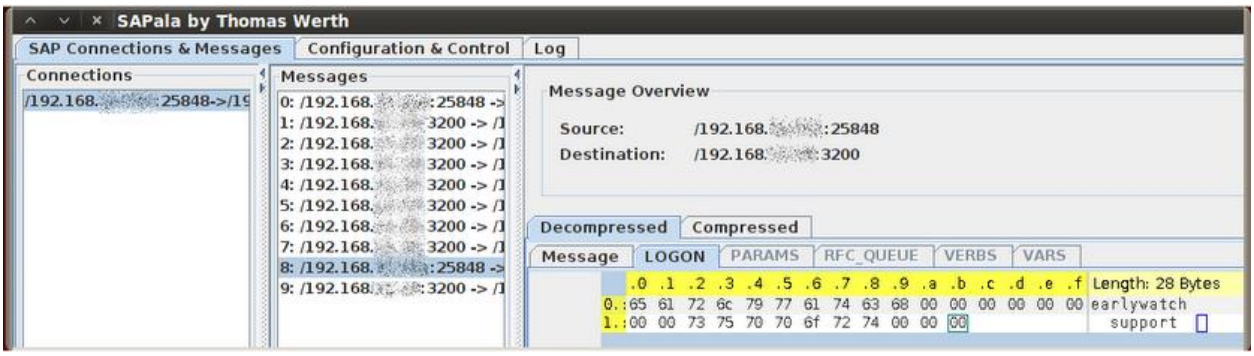
Ein periodischer Audit der verschiedenen RFC-Schnittstellen (SOAP, RFC, Registered RFC) hilft frühzeitig Einfallstore aufzuspüren und zu schließen.

Risiko unverschlüsselte Kommunikation

Die Kommunikation zwischen SAP und seinen Clienten kann mit geeigneten Werkzeugen wie dem Sniffer Wireshark abgefangen werden. Wer sich schon einmal die Mühe gemacht hat die Kommunikation von SAP in einem Sniffer anzusehen, hat im Allgemeinen nur Kauderwelsch sehen können. Dies hat zu der verbreiteten Annahme geführt, dass die Kommunikation von Client zu SAP nicht mitgelesen werden kann.

Dies ist jedoch nicht die ganze Wahrheit. Die Kommunikation erfolgt nur komprimiert, aber nicht verschlüsselt. Eine echte Verschlüsselung erhält man nur unter Einsatz von SNC. Hier wird der Inhalt mit privaten Schlüsseln abgesichert. Bei der komprimierten Übertragung gilt es lediglich den verwendeten Algorithmus in Erfahrung zu bringen, um die Kommunikation lesen zu können. Wie inzwischen bekannt ist der Algorithmus zur Dekomprimierung in dem Quellcode von MAXDB zu finden.

Das Programm SAPala zeigt deutlich Sichtbar die Schwächen einer unverschlüsselten Kommunikation auf. Das Programm kann die Kommunikation zwischen Client und Server dekodieren und Zugangsdaten herausfiltern. Auf dem Screenshot sieht man die Zugangsdaten zu einem EARLYWATCH Account.



Die Folgen des Verlusts von administrativen Zugangsdaten können bis hin zu schweren finanziellen Schäden reichen.

Daher sollte eine Verschlüsselung der Kommunikation mit SNC erfolgen. Die korrekte Konfiguration von SNC ist dabei turnusmäßig zu kontrollieren. SAP bietet die SNC-Verschlüsselung inzwischen kostenlos an, die reine Installation von SNC kann durch Drittanbieter schnell und kostengünstig erfolgen.

SAP Audits

SAP ist keine uneinnehmbare Festung - zumindest nicht ohne entsprechende Härtung. Da auf dem ERP System jedoch in der Regel die kritischen Unternehmensdaten liegen sollte das System gehärtet und regelmäßig auditiert werden. Dabei ist jedoch mehr als das Berechtigungskonzept zu prüfen. Die komplexen Prüfungen der verschiedenen SAP-Dienste wie RFC, WEB-GUI, SAP-Management-Konsole und mehr kann jedoch nur automatisiert durch ein spezialisiertes Programm (http://werth-it.de/auditor.html) erfolgen. Werth IT stellt speziell für die Allianz für Cybersicherheit eine kostenlose ACS-Version des SAP Security Scanners WERTH AUDITOR zur Verfügung. Diese im Funktionsumfang eingeschränkte Version kann genutzt werden, um einen ersten Überblick über die Sicherheit des eigenen SAP Systems zu erhalten. Das Programm kann mit einer formlosen E-Mail an mail@werth-it.de unter Angabe der eigenen Kontaktdaten und Unternehmensdaten kostenfrei angefragt werden. Das Programm wird nur Unternehmen mit Sitz in Deutschland zur Verfügung gestellt..

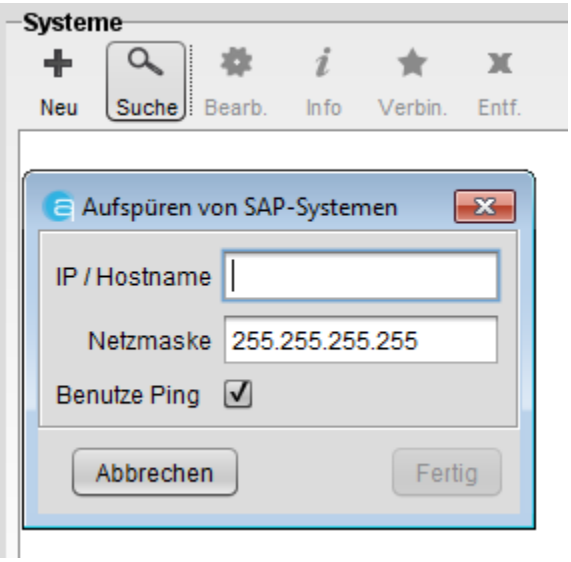
SAP Security Scanner - Werth Auditor

Installation

Die Installation erfolgt über die heruntergeladene “setup.exe” und ist in wenigen Schritten erledigt. Eine Programmregistrierung ist nicht erforderlich und das Programm kann direkt im Anschluss an die Installation gestartet werden.

Zielsysteme automatisch erfassen

Bevor die Systemprüfung beginnen kann, ist das Zielsystem dem Werth Auditor bekannt zu machen. Dies erfolgt durch Klick auf das “Suche”-Icon im Bereich “Systeme”.



(Nach einem Klick auf das “Suche”-Icon erscheint der Eingabedialog für die Ziel-Adresse des zu prüfenden SAP Systems.)

Es erscheint nun eine Eingabemaske mit der IP-Adresse des Zielsystems. Hat der Auditor ein SAP System erkannt folgt die Abfrage weiter Daten wie Name und SAP-System-ID. Zu jedem erkannten Dienst besteht nun die Möglichkeit Zugangsdaten für eine Prüfung zu hinterlegen oder den Dienst anonym prüfen zu lassen. Dies kann zu einem späteren Zeitpunkt jedoch jederzeit wieder geändert werden.

Das Zielsystem ist nun erfasst und kann auditiert werden.

Audit durchführen

Im Abschnitt “Test-Vorlagen” wählt man sodann eine geeignete Audit-Vorlage. Auf dem folgenden Screenshot ist die Auswahl “Kompletter Audit” sichtbar.

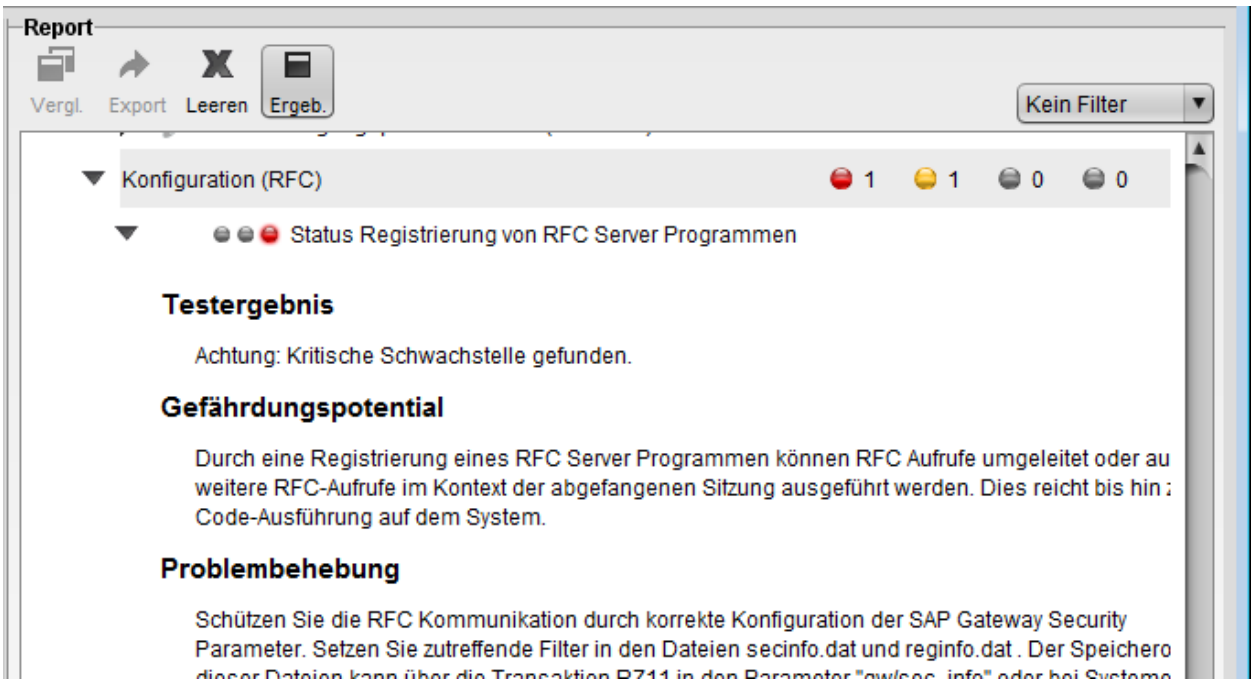
(Verfügbare Audit-Vorlagen)

Daraufhin aktiviert das Programm die in dieser Vorlage hinterlegten Tests. In der freien Version sind dies 30 Tests. Mit diesen Einstellungen wird sodann ein Audit über die Schaltfläche “Audit” mit dem bekannten Play Symbol gestartet.

Während der Audit läuft zeigt das Programm an welche Tests bereits ausgeführt wurden und welche noch nicht beendet sind. Anschließend stehen die Ergebnisse bereit.

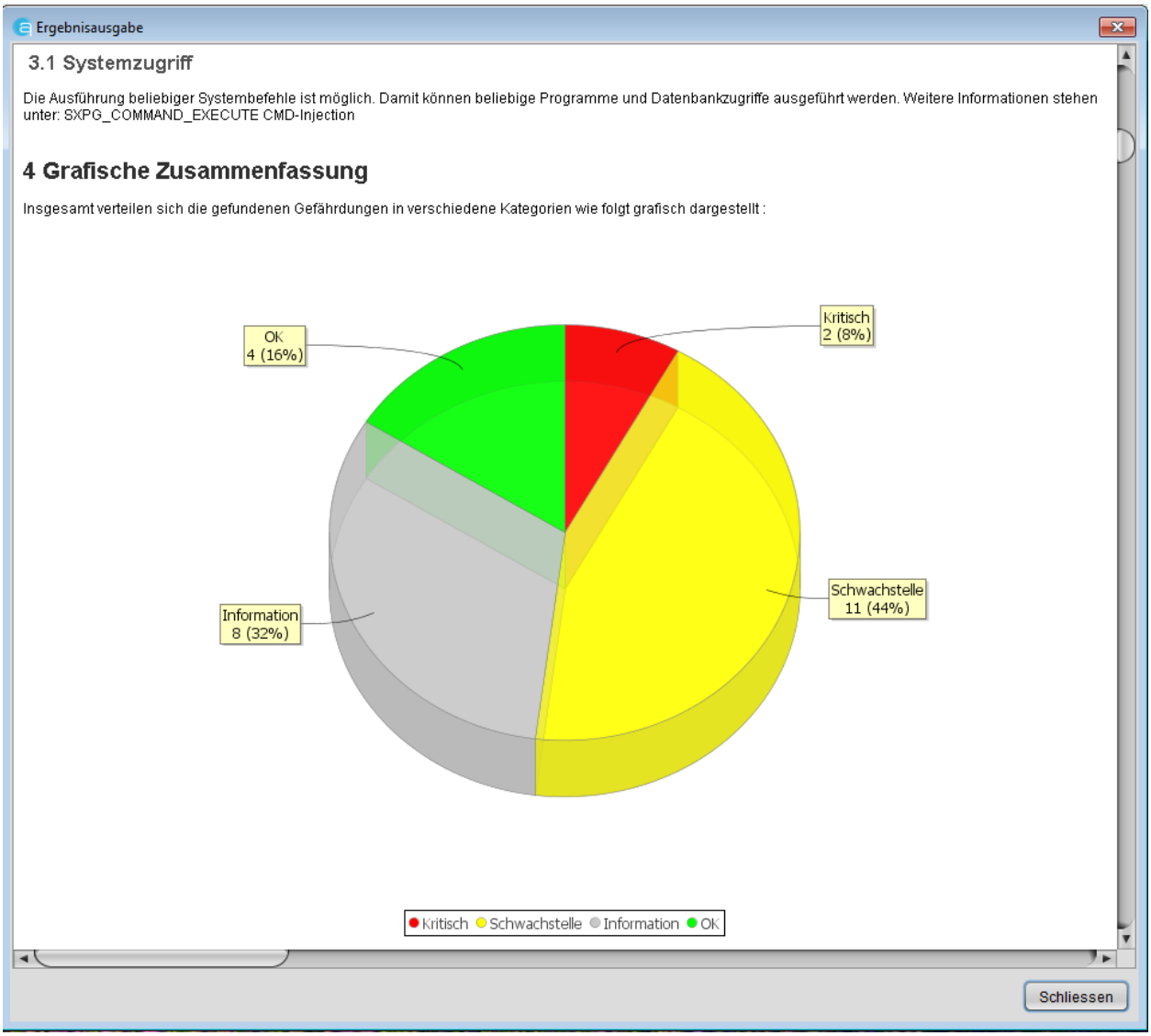
Ergebnis-Auswertung

Zu den einzelnen Tests erfolgt jeweils eine Bewertung des Ergebnisses mittels Ampel-System sowie eine Risikobeschreibung und eine Anleitung zur Problembehebung. Beispielhaft wird hier ein Testergebnis gezeigt, dass einen anonymen Systemzugriff ermittelt hat.



(Ergebnisanzeige zu einem Test mit kritischem Ergebnis)

Einen Bericht (PDF) kann man zu dem Audit mit dem Programm ebenfalls generieren lassen und sich direkt auch innerhalb des Programms eine Vorschau anzeigen lassen. Die Vorschau enthält sämtliche Test-Ergebnisse wie im obigen Screenshot dargestellt sowie eine Managementzusammenfassung und eine grafische Verteilung der Schwachstellen.



(Auszug aus der Vorschau des Auditberichts)

Weiterhin ist auch die Demonstration der gefundenen Risiken möglich. Hierzu kann mit der rechten Maustaste auf einen als kritisch markierten Test (Warndreieck) geklickt werden und im Popupmenü ein passender Exploit gestartet werden.
So hat man in wenigen Schritten und kürzester Zeit einen ersten Gradmesser für die Sicherheit des eigenen SAP-Systems.

Über Werth IT

Die Werth IT verfügt über führendes Know How in den Bereichen Softwareentwicklung und IT-Sicherheit. Dies konnte erfolgreich mit der Auszeichnung durch das Bundesministerium für Wirtschaft und Technologie mit dem Sonderpreis "IT-Sicherheit im Unternehmen" auf der Cebit 2014 unter Beweis gestellt werden.

Dieses Know How und unsere langjährige Erfahrung in diesen Bereichen nutzen wir zur Entwicklung innovativer und intuitiver Lösungen wie der einzigartigen Sicherheitslösung Werth Auditor für SAP Systeme.

Unsere Motivation ist der Schutz Ihrer Daten. Wir verfolgen das Ziel, dass Ihre Daten auch in Ihrem Unternehmen bleiben - genau da wo sie hingehören. Zusätzlich bieten wir zahlreiche Publikationen zu dem Thema IT-Sicherheit. So finden sich in diesem Bereich IT-Security Fachbücher, zahlreiche Fachartikel oder auch Security-Tools zur Sensibilisierung von IT-Risiken.

Ebenso ist uns die Verbesserung unserer Leistung sowie Kundenwünsche sehr wichtig. Haben Sie Anregungen oder Funktions-Wünsche für unsere Security-Lösung, zögern Sie nicht und kontaktieren uns mit Ihren Wünschen. Wir werden Ihre Vorschläge gern in dem nächsten Release berücksichtigen.

WERTH