GO OUT
entec
FORTINET
McAfee
wikima
IT-Security Forum #8
Computerworld.ch
Blickpunkt:KMU
maschinenbau

Hacking von SAP Systemen Schwachstellen, Angriffsszenarien, Gegenmassnahmen

Priska Altorfer, Managing Partner
Christian Schmid, Consultant
Sietze Roorda, Consultant

wikima4 AG
www.wikima4.com
Zug – Vevey – Scottsdale

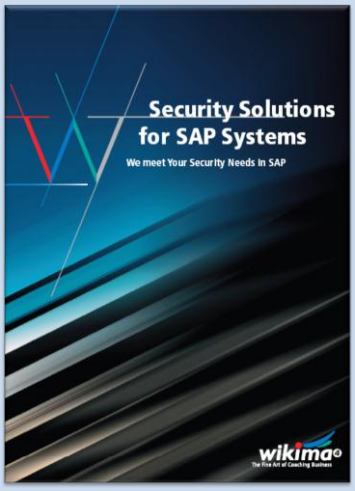
GO OUT
entec
FORTINET
McAfee
wikima
IT-Security Forum #8
Computerworld.ch
Blickpunkt:KMU
maschinenbau

Agenda

- Einführung
- Prozess Kontrollen
- Sniffing
- Access to sensitive Information
- Login & Password Cracking
- RFC Connections
- Database Hacking
- SAPLogon Cracker
- Q&A

GO OUT IT-SECURITY HOSTING
entec IT+COMMUNICATION
FORTINET
McAfee
wikima The Fine Art of Coaching Business
IT-Security Forum #8
Computerworld.ch
Blickpunkt:KMU
maschinenbau

Compliance Lösungen für SAP



GO OUT IT-SECURITY HOSTING
entec IT+COMMUNICATION
FORTINET
McAfee
wikima The Fine Art of Coaching Business
IT-Security Forum #8
Computerworld.ch
Blickpunkt:KMU
maschinenbau

(C) wikima4 2010

GO OUT IT-SECURITY HOSTING
entec IT+COMMUNICATION
FORTINET
McAfee
wikima The Fine Art of Coaching Business
IT-Security Forum #8
Computerworld.ch
Blickpunkt:KMU
maschinenbau

Sensible Daten sind wertvoll


$980-$4,900
Trojan to steal account information


$147
Birth certificate


$490
Credit Card Number with PIN


$98
Social Security card


$78-$294
Billing data


$6-$24
Credit card number


$147
Driver's license


$6
PayPal account logon and password

GO OUT IT-SECURITY HOSTING
entec IT+COMMUNICATION
FORTINET
McAfee
wikima The Fine Art of Coaching Business
IT-Security Forum #8
Computerworld.ch
Blickpunkt:KMU
maschinenbau

Agenda

- Einführung
- Prozess Kontrollen
- Sniffing
- Access to sensitive Information
- Login & Password Cracking
- RFC Connections
- Database Hacking
- SAPLogon Cracker
- Q&A

Prozess Kontrollen -
Gebiete von Hinterziehung und Betrug

Stammdaten	Lieferant	Kunde	Preis
•Material •Verkäufer •Kunde •Bank	•Mehrzahlung •Rabatt •Zahlungsbedingungen •Mengenquoten	•Kredit Limiten •Transport Schäden •Retour Sendungen •Beanstandungen	•Konditionen •Abläufe •Wechselkurs

Finanzen	Lager	Zahlungslauf	Konfiguration
•Perioden Buchungen •Buchungsdatum •Vermögens Registrierung Buchungen	•Lager Bewertung •Lager Verschiebungen •Inventar Zählung	•Spesen •Gradierung •Bonus Kategorie	•Basis Einstellungen •Genehmigungs- Matrix •Toleranz Werte

Prozess Kontrollen- Ein praktisches Beispiel

- Eine Kreditoren-Buchhalterin ist in Konflikt mit ihrem Ehemann geraten, der in der Einkaufsabteilung der gleichen Firma arbeitet. Er möchte, dass sie eine Rechnung an einen Lieferanten zahlt, obwohl diese nicht mit dem vereinbarten Rabatt übereinstimmt.
- Der fehlende Rabatt auf der Rechnung wird von beiden als gerechtfertigt angesehen, weil der Lieferant eine nicht voraussehbare Kostenexplosion im Rohmaterialbereich alleine tragen musste. Die Unterstützung durch den Abnehmer wurde dem Lieferanten verweigert.
- Ziel des Ehemannes ist es die gute Beziehung zum Lieferanten nicht zu gefährden dies im Hinblick auf weitere Vereinbarungen. Insbesondere zählt der Ehemann darauf, dass dieses Entgegenkommen ihm seinen eigenen Bonus der vom Erfolg von Lieferanten Verhandlungen abhängig ist auch in Zukunft gewährleistet bleibt.
- Betroffenes Betrugs Gebiet -> Lieferant, Finanzabteilung, Zahlungslauf

Prozess Kontrolle – Ein praktisches Beispiel (Ablauf)

- Der Lieferant schickt die Rechnung ohne den vereinbarten Rabatt;
- Die Kreditoren-Buchhalterin erfasst die Rechnung im SAP System;
- Die Rechnung wird wegen dem fehlenden Rabatt automatisch vom System blockiert;
- Die Kreditoren-Buchhalterin gibt die blockierte Rechnung zur Zahlung frei;
- Das Geld wird auf die Bank des Lieferanten überwiesen.

Prozess Kontrolle - Ein Praktisches Beispiel (IKS Report)

- Die Prozess Kontrolle „Freigabe von gesperrten Rechnungen“ läuft wöchentlich automatisch durch und wird dem Internen Verantwortlichen gemeldet:

Process control report - Release of blocked invoices

Company code	Invoice doc nr	Vendor code	Vendor name	Vendor country	Posted by	Posting date
1000	124/2010	9001	Casts Lee Ltd.	GB	MULLER	25/10/2010

Due date	Historical block?	Reason for block	Invoice status	Released by	Released on
24/11/2010	YES	Missing discount	Released	MULLER	25/10/2010

GO OUT IT-SECURITY HOSTING
entec IT+COMMUNICATION
FORTINET
McAfee
wikima The Fine Art of Coaching Business
IT-Security Forum #8
Computerworld.ch
Blickpunkt:KMU
maschinenbau

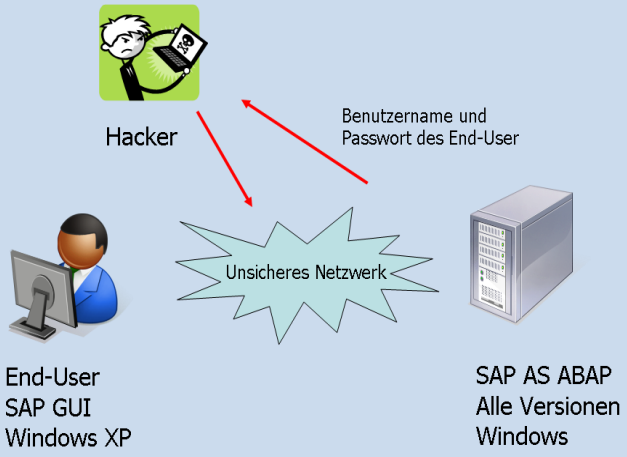
Prozess Kontrolle - Mangelnde Wahrnehmung von Indizien

IT-Security Forum #8

Agenda

- Einführung
- Prozess Kontrollen
- Sniffing
- Access to sensitive Information
- Login & Password Cracking
- RFC Connections
- Database Hacking
- SAPLogon Cracker
- Q&A

Sniffing



GO OUT
entec
FORTINET
McAfee
wikima
IT-Security Forum #8
Computerworld.ch
Blickpunkt:KMU
maschinenbau

Ausgangslage

- Ziel: Ein Buchhalter verfügt über eingeschränkte Berechtigungen (SOD Konflikte aufgelöst). Er kann Rechnungen erfassen, aber nicht freigeben.
- Prämisse: Er weiss, welche Mitarbeiter Rechnungen freigeben dürfen und kennt das Netzwerk und das SAP-System.
- Vorgehen: Er schliesst seinen privaten Laptop ans Netzwerk an und zeichnet den Datenverkehr auf.

Vorgehen: Sniffing der Daten

- Der Buchhalter hat sämtlichen Datenverkehr im Netzwerk aufgezeichnet und filtert die SAP-Verbindungen heraus
- Die Business-Daten sind nur schwer auswertbar, da sie in einer komplexen Struktur vorliegen, zudem möchte er Daten ändern, nicht lesen
- Der Hacker kann durch die Suche des Benutzernamens die Login-Sequenz auswerten

GO OUT
entec
FORTINET
McAfee
wikima
IT-Security Forum #8
Computerworld.ch
Blickpunkt:KMU
maschinenbau

Folgen der Aktion

- Das Opfer merkt vom Sniffing nichts
- Der Angreifer muss lediglich nach dem Benutzernamen des Chefbuchhalters suchen und kann sein Passwort danach auslesen
- Mit dem Passwort des Chefbuchhalters kann er seine fiktive Rechnung freigeben und sich bereichern
- In den Protokollen wird der Benutzername des Chefbuchhalters auftauchen

Weiteres Vorgehen

- Der Buchhalter analysiert die Berechtigungen des Chefbuchhalters weiter
- Er erkennt, dass dieser, für den Export der ESR-Zahlungen auf die Kommandozeile zugreifen darf
- Es ist möglich Benutzer auf dem lokalen SAP-Server zu erstellen
- Damit installiert er Programme auf dem Server um die Passwörter zu knacken

IT-Security Forum #8

Agenda

- Einführung
- Prozess Kontrollen
- Sniffing
- Access to sensitive Information
- Login & Password Cracking
- RFC Connections
- Database Hacking
- SAPLogon Cracker
- Q&A

IT-Security Forum #8

Vorgehen: Ausführen von Kommandos

- Der Angreifer erstellt sich einen lokalen Benutzer auf dem SAP-Server und vergibt diesem lokale Administratorenrechte.
- Er loggt sich auf der Konsole des SAP-Servers ein
- Der Hacker hofft, dass Windows-Passwörter auch auf den SAP-Systemen verwendet werden

IT-Security Forum #8

Agenda

- Einführung
- Prozess Kontrollen
- Sniffing
- Access to sensitive Information
- Login & Password Cracking
- RFC Connections
- Database Hacking
- SAPLogon Cracker
- Q&A

IT-Security Forum #8

Vorgehen: Cracking der Passwörter

- Die verschlüsselten Passwörter werden lokal auf den Laptop des Hackers kopiert
- Die Passwörter sind innerhalb weniger Minuten geknackt und im Klartext ersichtlich
- Es handelt sich um die Windows-Passwörter, diese sind aber oft mit SAP-Passwörtern identisch

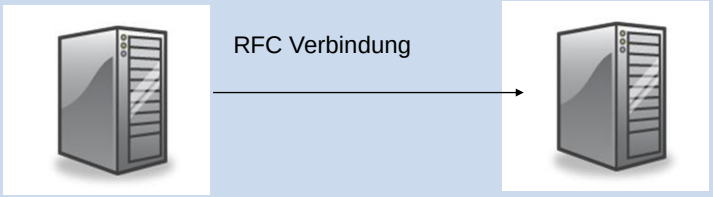
ID	USERNAME/LMHASH	LMpasswd1	LMpasswd2	NTpasswd
1025	Apolkis	HIPHOP_		HipHop_
1030	Bagwell	#SONY2M	$#	#sOny2M$#
1026	Bellick	1AMTHEB	0SS	1amthebOss

GO OUT
entec
FORTINET
McAfee
wikima
IT-Security Forum #8
Computerworld.ch
Blickpunkt:KMU
maschinenbau

Agenda

- Einführung
- Prozess Kontrollen
- Sniffing
- Access to sensitive Information
- Login & Password Cracking
- RFC Connections
- Database Hacking
- SAPLogon Cracker
- Q&A

Szeanario 2: RFC Hacking



Ausgangslage

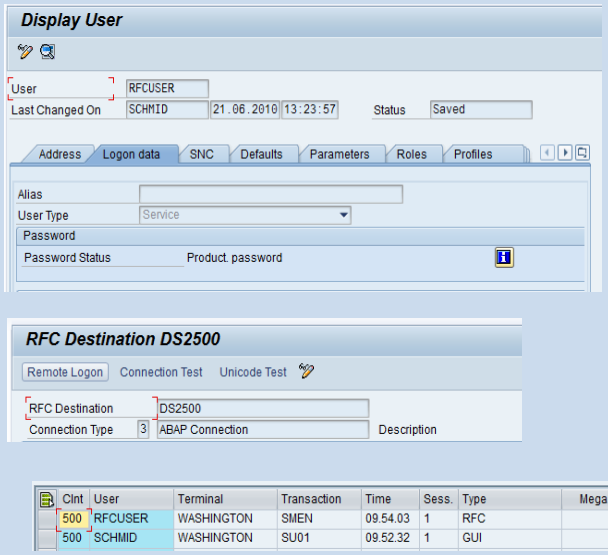
- Ein Entwickler verfügt über volle Rechte auf dem HCM-Entwicklungssystem, darf sich aber nicht am produktiven System anmelden.
- Das Entwicklungssystem enthält keine kritischen HR-Daten, an welchen er interessiert ist
- Er sucht sich einen Zugang zum produktiven System

RFC Benutzer

- RFC Benutzer dienen zum Austausch von Daten zwischen zwei SAP-Systemen
- Diese führen auf dem Zielsystem gewissen Funktionen aus (Remote Function Call)
- Normalerweise verfügen sie über eingeschränkte Berechtigungen und dürfen sich nicht via SAPGUI einloggen
- Temporär werden manchmal höhere Rechte vergeben (z.B. bei einer Migration)

GO OUT
entec
FORTINET
McAfee
wikima
IT-Security Forum #8
Computerworld.ch
Blickpunkt:KMU
maschinenbau

RFC User als Dialog



Szenario: Kopieren der Daten

- Der Hacker meldet sich mit einem der geknackten Passwörter an.
- Dieser Account verfügt über vollen Zugriff, inklusive Gehaltsdaten (Kundendaten, Materialstamm).

Pay grade level	Name	Mean value	Currency	Salary	Currency	Compa-ratio
02	Mr. John Powell	62.950,00	CAD	60.000,00	CAD	0,95
	Mr. Edward Downey	62.950,00	CAD	60.750,00	CAD	0,97
01	Mr. Dennis West	78.500,00	CAD	76.000,00	CAD	0,97
03	Mrs Jane Russell	94.000,00	CAD	70.000,00	CAD	0,74
01	Mrs Sharron Russell	115.000,00	CAD	106.943,00	CAD	0,93
	Mr. Peter Thompson	87.000,00	CAD	83.400,00	CAD	0,96
	Mrs Wilma O'Brien	87.000,00	CAD	84.500,00	CAD	0,97
02	Mr. Denis Sutton	93.500,00	CAD	95.670,00	CAD	1,02
03	Mr. Pierre Couturier	0,00	CAD	36.000,00	CAD	0,00
08	Mrs Joanne Westin	0,00	CAD	39.600,00	CAD	0,00

GO OUT
entec
FORTINET
McAfee
wikima
IT-Security Forum #8
Computerworld.ch
Blickpunkt:KMU
maschinenbau

Agenda

- Einführung
- Prozess Kontrollen
- Sniffing
- Access to sensitive Information
- Login & Password Cracking
- RFC Connections
- Database Hacking
- SAPLogon Cracker
- Q&A

Datenbank

Hacker

Database
MSDE
Windows

SAP AS ABAP
Any Version
Any OS

GO OUT
entec
FORTINET
McAfee
wikima
IT-Security Forum #8
Computerworld.ch
Blickpunkt:KMU
maschinenbau

Ausgangslage

- Ziel: Ein Datenbank-Administrator möchte Daten aus einem SAP-System kopieren, auf welches er keinen Zugriff hat.
- Vorgehen: Er kann die Daten entweder direkt aus dem einzelnen Tabellen auslesen oder sich interaktiv am System anmelden.

Berechtigungen für Datenbanken

- SAP greift mit einem dedizierten Benutzer auf die Datenbank zu, welche volle Berechtigungen besitzt.
- Die Rechte auf dem Datenbankserver werden nicht im SAP-System angezeigt. Änderungen auf Ebene Datenbank erscheinen ebenfalls nicht in den Logs von SAP.
- MS SQL und Oracle: Berechtigungen durch zugewiesene Gruppen (Lokal oder AD)

IT-Security Forum #8

Möglichkeiten

- Lesen und Ändern von beliebigen Daten ohne Protokolle auf dem Server
- Temporäre Änderungen von Passwörtern
- Ausschalten des Audit Trails
- Löschen oder Manipulation der Protokolle
- Datenbank herunterfahren

IT-Security Forum #8

Berechtigungen für Datenbanken

- SAP greift mit einem dedizierten Datenbank-Benutzer auf diese zu. Dieser Benutzer kann alle Tabellen lesen und ändern.
- Die Rechte auf dem Datenbankserver werden nicht im SAP-System verwaltet. Änderungen auf Ebene Datenbank erscheinen ebenfalls nicht in den Logs von SAP. Das Logging auf der Datenbank muss explizit eingeschaltet werden.
- MS SQL und Oracle: Berechtigungen durch zugewiesene Gruppen (Lokal oder AD)

IT-Security Forum #8

Möglichkeiten

- Lesen und Ändern von beliebigen Daten ohne Protokolle auf dem Server
- Temporäre Änderungen von Passwörtern
- Ausschalten des Audit Trails
- Löschen oder Manipulation der Protokolle
- Datenbank herunterfahren

IT-Security Forum #8

Lesen von Daten

- Die Namen der Tabellen müssen bekannt sein, sind aber mit SAP Kenntnissen einfach zu erfahren.
- Mehrere Tabellen sind nötig, um ein vollständiges Bild zu erhalten (Fremdschlüssel) -> Feld BVTYP
- SAP sieht keine Verschlüsselung (Gehaltsdaten) vor

```
SELECT * FROM LFBK
```

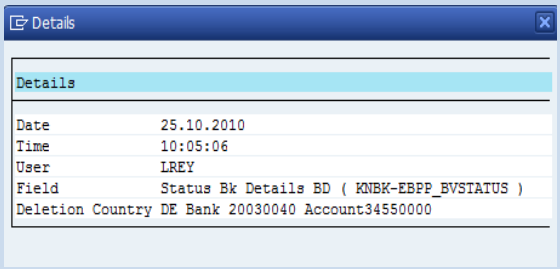
INS Ln 1, Col 19

	MANDT	LIFNR	BANKS	BANKL	BANKN	BKONT	BVTYP	XEZER	BKREF	KOINH
8	800	0000000200	DE	23022200	98765896					
9	800	0000000300	DE	20050000	8484636			X		
10	800	0000001000	DE	10050033	90010000		0001			
11	800	0000001000	DE	19652993	10003299		0002			

GO OUT
entec
FORTINET
McAfee
wikima
IT-Security Forum #8
Computerworld.ch
Blickpunkt:KMU
maschinenbau

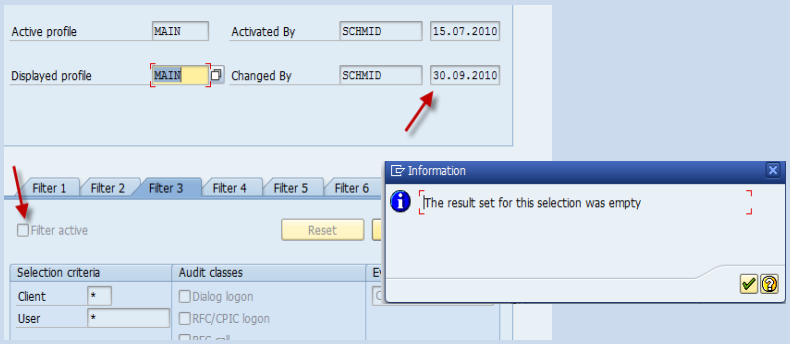
Temporäre Änderung von Passwörtern

- Passwort eines Benutzers wird temporär geändert.
- Kein Eintrag in den SAP Logfiles (Audit Log, Tabellenlog)
- Benutzername des «Opfers» erscheint in den Logfiles



Ausschalten des Audit Trails

- Audit Log kann mit einem Tool ausgeschaltet werden, um keine Spuren während den böswilligen Aktionen zu hinterlassen.
- Kein interaktives Login am System nötig.



GO OUT
entec
FORTINET
McAfee
wikima
IT-Security Forum #8
Computerworld.ch
Blickpunkt:KMU
maschinenbau

Manipulation der Änderungsbelege

- Kritische Änderungen werden im SAP-System protokolliert (z.B. Änderung Kontodaten)
- Werden die richtigen Daten auf dem SQL-Server geändert, können die Protokolle gefälscht werden.
- Änderungen sind mit einem Risiko verbunden, da Fehler die Stabilität des SAP-System gefährden können.

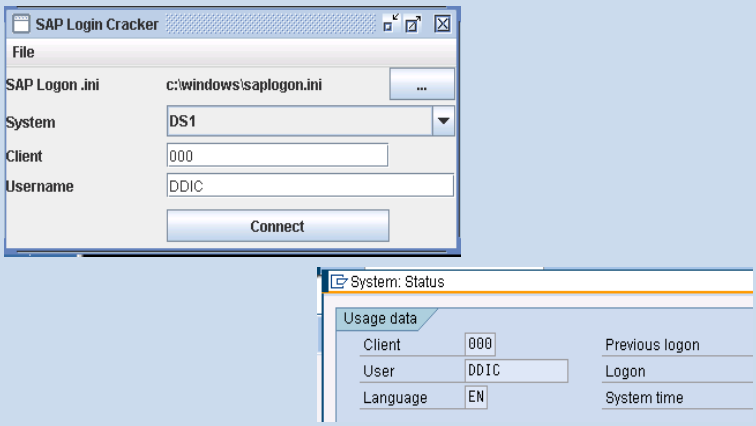
Agenda

- Einführung
- Prozess Kontrollen
- Sniffing
- Access to sensitive Information
- Login & Password Cracking
- RFC Connections
- Database Hacking
- SAPLogon Cracker
- Q&A

GO OUT
entec
FORTINET
McAfee
wikima
IT-Security Forum #8
Computerworld.ch
Blickpunkt:KMU
maschinenbau

SAPLogon Cracker

- Single Sign on – für jeden Benutzer ☺



Gegenmassnahmen

- Verschlüsselung des Datenstroms zwischen SAPGUI und SAP-Server (SNC) mit zum Beispiel AdNovum SecStack
- Sichere Konfiguration des SAP-Servers, inklusive Betriebssystem
- Implementierung eines Berechtigungskonzepts
- Monitoring mit mesaforte™ (wikima4)
- Zugangskontrolle für Gebäude einführen und Mitarbeiter entsprechend schulen

Zusammenfassung

Wichtig für die Geschäftsleitung

- Daten in ERP Systeme müssen aktiv geschützt werden
- Kontinuierliches Monitoring versus jährliche Überprüfung
- ERP Schutz Möglichkeiten nutzen, einstellen und pflegen

Wichtig für die IT

- Komplexe ERP Systeme verlangen einen integrierten Ansatz
- Flexibilität geht auch mit Sicherheit und Compliance
- Stufenweises Vorgehen versus Big Bang

Wichtig für die Benutzer

- Schutz der Mitarbeiter durch weniger Rechte
- Automatisieren der manuellen Kontrollen
- Missbraucht werden können auch Benutzer Id‘s

142

GO OUT IT-SECURITY HOSTING
entec IT+COMMUNICATION
FORTINET
McAfee
wikima4 The Fine Art of Coaching Business

IT-Security Forum #8

Computerworld.ch
Blickpunkt:KMU
maschinenbau

Priska Altorfer
Managing Partner

Christian Schmid
Sietze Roorda
Consultant

wikima4 The Fine Art of Coaching Business

wikima4 AG
Bahnhofstrasse 28 / 6304 Zug / Switzerland
T: +41 (0)41 711 94 54 / F: +41 (0)41 711 96 54
mail@wikima4.com / www.wikima4.com