WERTH

WERTH auditor
sicherheit für sap-systeme

SAP-Sicherheit

für CI(S)Os

Autor: Thomas Werth

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

Was ist SAP?

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 werden üblicherweise von SAP-Systemen abgedeckt:

- 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)

Warum ist ein SAP-System so „wertvoll“?

SAP-Systeme verarbeiten und speichern die unternehmenskritischen Daten. In diesem System finden sich die Kunden-, Lieferanten- und Personaldaten. Ebenso werden hier die Finanzdaten wie Bilanzen, Bankkonten und Buchungen verarbeitet. Zusätzlich trifft man Planungsdaten, Konstruktionsdaten und Vertriebsinformationen wie Preislisten an. Jeder einzelne Datenbereich ist bereits sensibel und in Kombination hoch kritisch. Ein Ausfall des Systems und ein ausbleibender Zugriff auf diese Daten bei gleichzeitigem Verarbeitungsstillstand führen in der Regel zu einem Betriebsausfall.

Damit sind SAP-Systeme ein lohnendes Ziel für Cyber-Angriffe. Egal ob Spionage, Sabotage oder Betrug die Motivation ist, die Daten in dem SAP-System geben ein attraktives Ziel ab. Cyberattacken auf SAP-Systeme können großen Schaden im Unternehmen verursachen. Um sich wirkungsvoll vor ihnen zu schützen, sollten Sie wissen, welche Motive professionelle Hacker verfolgen, wie Sie sich Zugang in das Herz Ihres Unternehmens verschaffen und welche Folgen ein Hackerangriff haben kann.

Das "Problem" Cyberkriminalität ist den meisten Unternehmen natürlich bewusst. Das Thema wird jedoch erstaunlicherweise nur selten dem Stellenwert eines SAP-Systems gerecht. Das Berechtigungskonzept in Kombination mit Standard-Schutzmaßnahmen wie ein Betrieb des Systems im Intranet und eine externe Firewall werden bisher allgemein als ausreichend angenommen. Diese Maßnahmen sind natürlich auch notwendig, doch reichen sie nicht aus um speziell auf SAP-Systeme abgestimmte Angriffe zu unterbinden.

Wenn Sie Ihr SAP-System zuverlässig vor gezielten Cyberangriffen schützen möchten, müssen Sie die Angriffswege kennen und prüfen ob Ihre vorhandenen Sicherheitsmaßnahmen und -einstellungen diese stoppen.

Sicherheit ist dabei als fortlaufender Prozess anzusehen und unterliegt ständig neuen Erkenntnissen und Anforderungen.
Daher ist ein kontinuierlicher Austausch zu diesem Thema ein wichtiger Aspekt, um sein Wissen aktuell zu halten.

Hintergrundinformationen zu Cyberangriffen

Die Sicherheit von SAP-Systemen kann nicht isoliert betrachtet werden. Es ist notwendig auch das Netzwerk und die Infrastruktur zu beleuchten. Somit ist es ebenfalls von Bedeutung mit den Eigenschaften und den Ablauf von modernen Cyberattacken vertraut zu sein, da diese als Basis einer Attacke auf ein SAP-System dienen können.

Eigenschaften moderner Cyberattacken

Der Wert der von Unternehmen erzeugten und gespeicherten Daten steigt täglich. Entsprechend steigen die Zahlen der Cyberkriminalität. Angreifer sind immer professioneller, besser ausgestattet und finanziert. Ein Angriff erfolgt gut vorbereitet und vor allem schnell und geräuschlos. Cyberangriffe haben dabei drei wesentliche Charaktereigenschaften:

1. Sie sind absolut **Zielgerichtet** und der Angriff ist perfekt auf das Opfer abgestimmt.
2. Sie sind **persistent**. Wenn ein Unternehmen einmal infiltriert ist, bleibt der Angreifer solange er will und kann jederzeit zurückkehren.
3. Die Angreifer agieren im **Verborgenen**, um eine Entdeckung zu vermeiden.

Selbst ausgefeilte Abwehrmaßnahmen wie Next-Generation Firewalls und hochentwickelte Antiviren Lösungen halten entschlossene Angriffe nicht auf. Oft werden die Angriffe erst nach Monaten erkannt und es sind schon viele Daten abgeflossen. Auch vermeintliche Hoch-Sicherheitssysteme stellen keine uneinnehmbare Festung dar wie die Angriffe auf den deutschen Bundestag [9] oder den Antivirenhersteller Kaspersky [10] eindringlich bewiesen haben.
Letztlich sind damit alle Systeme des Opfers für die Angreifer im Zugriff – auch die SAP-Systeme.
Um zu ermitteln wer hinter einem Angriff steckt, muss man zunächst die Arten und Gründe der Angriffe in Erfahrung bringen:

WER dringt in SAP-Systeme ein und welche Arten von Cyberkriminalität existieren?

Wirtschaftsspionage >> Wirtschaftsspionage ist eine reale Bedrohung. Dennoch treffen fast ein Drittel der mittelständischen Unternehmen keine Maßnahmen im Bereich IT-Sicherheit und Datenschutz. Im KMU-Bereich herrscht die Annahme vor, dass Wirtschaftsspione kein Interesse an ihren Daten haben. In der Realität fischen Spione jedoch global alle Daten ab und werten diese dann später nach Interessantem Material ab, so der DHB. Darunter befinden sich auch Sensible Kunden- und Mitarbeiterdaten sowie Rechnungen, Angebote, Verträge, usw.

Industriespionage >> Die Industriespionage wurde bislang unterschätzt, so der VDI. Gerade deutsche Unternehmen mit ihren Nischeninnovationen bieten für Spione hochinteressante Ziele. Nicht auszumalen was es für eine deutsche Firma bedeutet, wenn ein gerade patentiertes Bauteil noch vor Markteinführung eins zu eins von einem chinesischem Verkäufer auf einer Messe angeboten wird. Im allerschlimmsten Fall kann der Verlust bzw. die Kopie von Know-how ein betroffenes Unternehmen in die Insolvenz führen.

Datenmanipulation >> Täuschung mit Methode. Unter Datenmanipulation versteht man das Verändern, Hinzufügen oder Löschen von Daten in einer Datenbank. Die Motivation der Hacker ist vielfältig. Sie reicht vom Spaß am Chaos, wie bei den Hacker-Attacken auf Visa, Master Card und PayPal 2011 über die Herausforderung Sicherheitslücken ausfindig zu machen und als Erfolg zu verbuchen bis hin zu betrügerischen Absichten. Daten werden z.B. bewusst verändert, um das dahinterstehende Unternehmen zu schädigen und dem eigenen einen Vorteil zu verschaffen. Doch die Bedrohung sitzt nicht immer an einem externen Rechner in Übersee. Deshalb ist es wichtig das Berechtigungskonzept des SAP-Systems zu analysieren und festzulegen wer intern Zugriff auf bestimmte Bereiche haben darf sowie mögliche Schwachstellen zur Umgehung des Berechtigungskonzeptes aufzuspüren.

Datendiebstahl >> Manager melden ein immer größeres Risiko für Cyber-Attacken. Deutsche Unternehmen sind einer wachsenden Bedrohung von Datenklau-Attacken aus dem Ausland ausgesetzt. Betrüger versuchen immer wieder bei ahnungslosen Unternehmen sensible Daten, wie Passwörter, geistiges Firmeneigentum, Email-Adressen, Kundendaten oder Geld zu erbeuten. Oft wird der Verlust der Daten wenn überhaupt erst bemerkt, wenn es längst zu spät ist. Der Großteil der Unternehmen hält jedoch noch immer einen Hacker-Angriff für unwahrscheinlich. Die Hauptbegründung liegt nach einer Umfrage von EY darin, dass sich diese Unternehmen durch ihr SAP-System ausreichend geschützt fühlen. Tatsächlich handelt es sich bei den meisten

Sicherheitsvorkehrungen jedoch um Standardeinstellungen, die für routinierte Hacker kein Hindernis darstellen.

Welche Beweggründe treiben Hacker an?

Den benannten Bedrohungen lassen sich nun potentielle Quellen zuordnen.
Die Quelle für **Wirtschaftsspionage** ist jedoch zumeist staatlicher Natur. Aufgedeckte Cyberoperationen haben hier belegen können, dass China, USA, Russland und auch der Iran gezielt Informationen zur Stärkung ihrer eigenen Wirtschaft sammeln [3].
Industriespionage hingegen wird meist von zwielichtigen Konkurrenzunternehmen begangen oder in Auftrag gegeben, der Weg kann hier auch zur organisierten Kriminalität zeigen. Finanzielle Motive sind hier prägend.
Datenmanipulation fällt meist auf unzufriedene Mitarbeiter zurück, die entweder Frust abbauen oder sich bereichern wollen. Hierzu lassen sich jedoch auch Hacker-Angriffe zählen, die mitunter durch Manipulation das komplette SAP-System lahmlegen können [2].
Der **Datendiebstahl** ist oftmals das Ergebnis obiger genannter Angriffe und ist je nach Art der Daten entsprechend den potentiellen Angreifern zuzuordnen.

Ausführung eines modernen Cyberangriffs

Informationen sind die Währung des 21. Jahrhunderts. Daher sind Unternehmensdaten verstärkt zum Ziel staatlicher und krimineller Aktivitäten geworden. Viele Unternehmen glauben sich jedoch in Sicherheit, da doch "niemand" Interesse an Ihren Daten haben sollte und Ihre digitalen Herzen -die SAP-Systeme- doch im sicheren Intranet stehen. Dieser Irrglauben kann sehr gefährlich sein. Zeigt doch die aktuelle Studie der Bitkom, dass allein in Deutschland 2014 jedes zweite Unternehmen digitalen Angriffen ausgesetzt war. Weiterhin nimmt die Vernetzung der SAP-Systeme drastisch zu (Cloud, Mobile, Web-Anwendungen). Doch selbst ein Zugriff auf die SAP-Systeme im "sicheren" Intranet ist für professionelle Angreifer keine Herausforderung. Solche hochmodernen Angriffe - auch Advanced Persistent Threads (APT) genannt - laufen in der Regel nach folgendem Muster ab:

Cyberangriff in 6 Schritten:

1. Der Angreifer erlangt über eine Phishing E-Mail / Webseite oder Netzwerk- bzw. Anwendungsschwachstelle die Kontrolle über einen Computer in dem Unternehmensnetzwerk und schleust auf diesem Weg Malware ein und infiltriert das Unternehmen.

2. Die Malware erkennt automatisch weitere Zugangsmöglichkeiten und Schwachstellen im Netzwerk und kommuniziert über verdeckte Kanäle durch die Unternehmensfirewall hindurch mit dem Angreifer, um neue Befehle und weitere Schadprogramme zu laden.

3. Der Angreifer platziert zusätzliche Hintertüren, um seinen Zugriff auf das Unternehmen "zu sichern"

4. Über den Zugang zu dem Unternehmensnetzwerk sammelt der Angreifer nun die gewünschten (Zugangs-)Daten und kann so auch auf die Unternehmensserver zugreifen, Daten suchen und abgreifen.

5. Die Daten werden auf dem infiltrierten System zusammengefasst und anschließend über den verdeckten Kanal an den Angreifer gesendet.

6. Spuren und Hinweise auf den Cyberangriff werden von dem Angreifer beseitigt. Jedoch bleibt das Unternehmen weiter infiltriert und der Angreifer kann jederzeit zurückkehren, um weitere Daten zu stehlen.

Ein nachvollziehbares Beispiel für einen solchen Angriff ist hier zusammen gefasst [7] . Jedenfalls sollte jedem Unternehmen bewusst sein, dass ab Punkt 4. ein Zugriff auf die SAP-Systeme im Intranet für externe Angreifer möglich ist. An dieser Stelle kann ein Zugriff mit erbeuteten Zugangsdaten oder bekannten Schwachstellen erfolgen. Allein 2014 hat SAP mehr als 390 Sicherheitspatches veröffentlich, von denen mehr als 46% mit hoher Priorität gekennzeichnet sind. Teilweise sind die Angriffswege im Internet zu finden und somit auch von unerfahrenen Angreifern erfolgreich durchführbar.

Angriffswege auf SAP-Systeme

Versetzt man sich nun in die Situation, dass ein Cyber-Angriff auf ein Unternehmensnetzwerk erfolgreich war, gilt es den Blickwinkel des Angreifers einzunehmen.
Welche Wege stehen ihm nun zur Verfügung um Zugriff auf ein SAP-System zu erhalten oder seinen Zugriff in der SAP-Landschaft auszubauen?
Hier gibt es bekannte Angriffswege mit denen Zugang zu einem System erlangt werden kann sowie weitere mit denen der Zugang im System und zu weiteren SAP-Systemen ausgebaut werden kann. Die Punkte 1-5 stellen in der Regel einen Einstieg in ein System dar. Oftmals wird hier aus Sicht eines Angreifers mit einem weniger gesicherten System wie einem Entwicklungssystem gestartet. Ist der Zugang erst einmal etabliert werden die Punkte 6-9 genutzt, um den Zugriff zu erweitern.

1**. Unsichere Konfigurationen** des SAP RFC Gateways ermöglichen Angreifern das Ausführen beliebiger Systemkommandos unter dem Service-Benutzer des SAP-Systems, was auch einen Zugriff auf die Datenbank ermöglicht.

2. Unveränderte **Standard-Zugangsdaten** ermöglichen Angreifern direkten Systemzugriff.

3. **Unverschlüsselte Kommunikation**: Wird auf eine verschlüsselte Kommunikation (SNC) verzichtet, lassen sich die Zugangsdaten im Klartext im Netzwerk abfangen.

4. **Technische Schwachstellen** in aus dem Netzwerk erreichbaren Schnittstellen. So erlauben Schwachstellen in dem J2EE Portalservers ohne Zugangsdaten das Anlegen beliebiger Benutzer. Solche Systeme sind oft an das Internet angebunden und lassen sich sogar mittels Google-Suche aufspüren.

5. **Schwache Passwortrichtlinien** begünstigen Passwort-Rate-Angriffe, so kann ein Angreifer durch Ausprobieren Systemzugang erhalten.

6. **Ausnutzung von Vertrauensstellungen**: Den Zugang von einem weniger sicheren System (Entwicklungssystem) auf ein produktives System erweitern. Dazu können Trusted RFC Verbindungen, die im weniger sicheren System zu dem produktiven System konfiguriert sind, genutzt werden. Ein Angreifer kann über die Transaktion SE16 in Erfahrung bringen, welche RFC Destinationen konfiguriert sind und dann über die SM59 eine Verbindung herstellen. Auf dem Zielsystem kann er dann unter anderem über die SE37 beliebige weitere Funktionen ausführen.

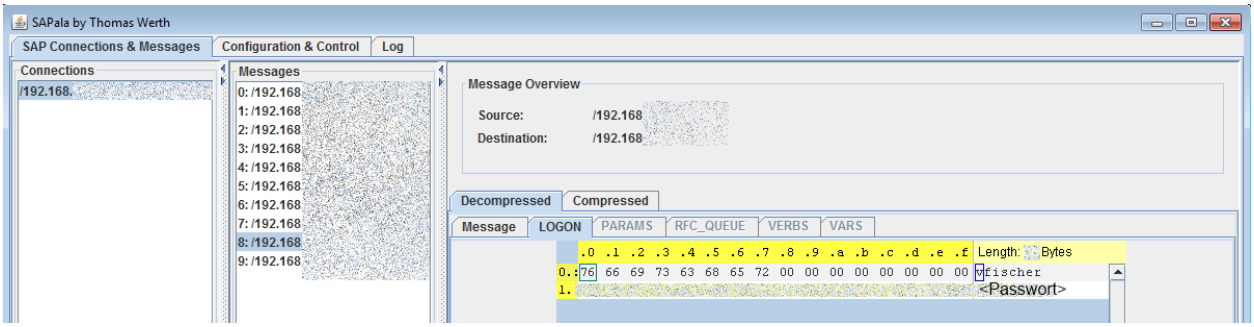
7. **Kritische Berechtigungskombinationen** lassen sich auch für kriminelle Handlungen verwenden, beispielsweise unautorisierte Finanztransaktionen oder die Zuweisung privilegierter Rechte im System.

8. **Fehlende oder unzureichende Berechtigungsprüfungen** können das Aufrufen von Systemfunktionen ermöglichen, die nur von einem bestimmten Personenkreis aufrufbar sein sollten.

9. **Eigene ABAP-Programme** können Hintertüren enthalten. Beispielsweise zur Umgehung der Mandantentrennung, Systembefehle aus zu führen oder an allen SAP-Sicherheitsvorkehrungen vorbei auf die Datenbank zu zugreifen. Manchmal fehlen hier auch schlicht die Berechtigungsprüfungen und sensible Programme dürfen von jedem Benutzer gestartet werden.

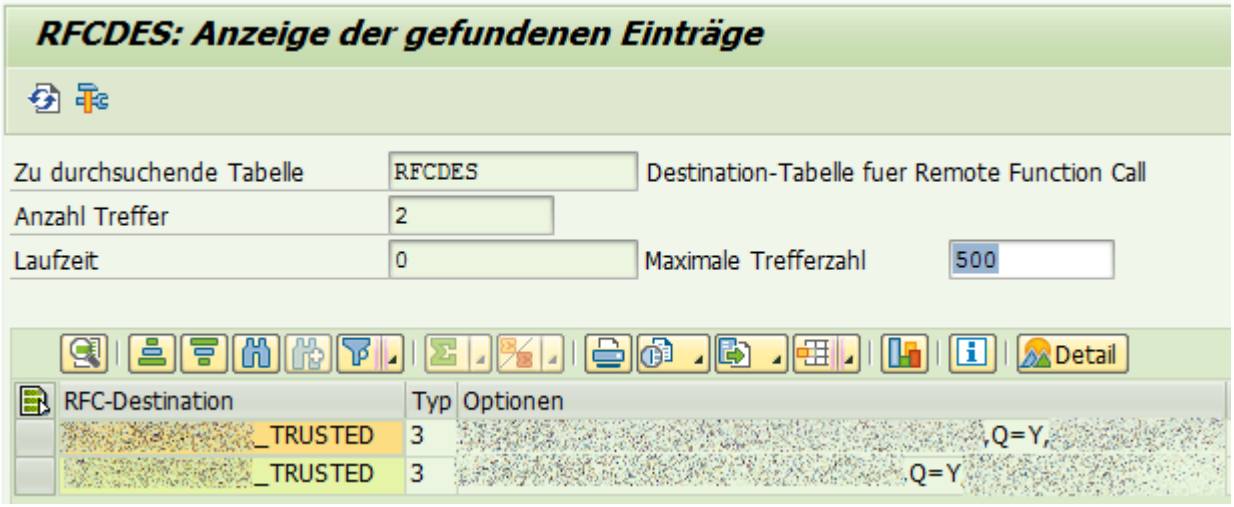
Beispiel eines Cyberangriffs mit Ziel SAP-System

Der beste Weg die beschriebenen Angriffswege zu verstehen, ist einen fiktiven Angriff zu visualisieren. Hierzu soll ein Windows-Trojaner, welcher SAP-Systeme ausspioniert [11], als Grundidee fungieren. Ein moderner Cyber-Angriff war erfolgreich, die Unternehmensfirewall wurde überwunden, die Antivirenlösung getäuscht und man befindet sich auf einen beliebigen Mitarbeiter-PC. Im Zielnetzwerk erfolgt keine verschlüsselte Kommunikation (SNC) zwischen den Nutzern und dem SAP-System. Dies wird in diesem Szenario ausgenutzt und der Datenverkehr zwischen den Benutzern und dem System wird im Netzwerk abgefangen, mit dem Ziel Zugangsdaten zu erspähen.
Damit beginnt der Angriff auf das SAP-System mit Punkt 3 „unverschlüsselte Kommunikation“ aus obiger Liste (Bild 1).



(Bild 1: Abgefangene Login Daten für ein SAP-System werden im Klartext angezeigt).

Die Zugangsdaten gelten in diesem Szenario jedoch nur für ein nicht produktives System. Daher folgt der nächste Schritt mit Punkt 6 „Ausnutzung von Vertrauensstellungen“. Der Angreifer loggt sich in das System und sucht in der Tabelle RFCDES nach „Trusted RFC-Destinationen“. Diese erkennt er an dem Typ 3 und der Option Q=Y (Bild 2).

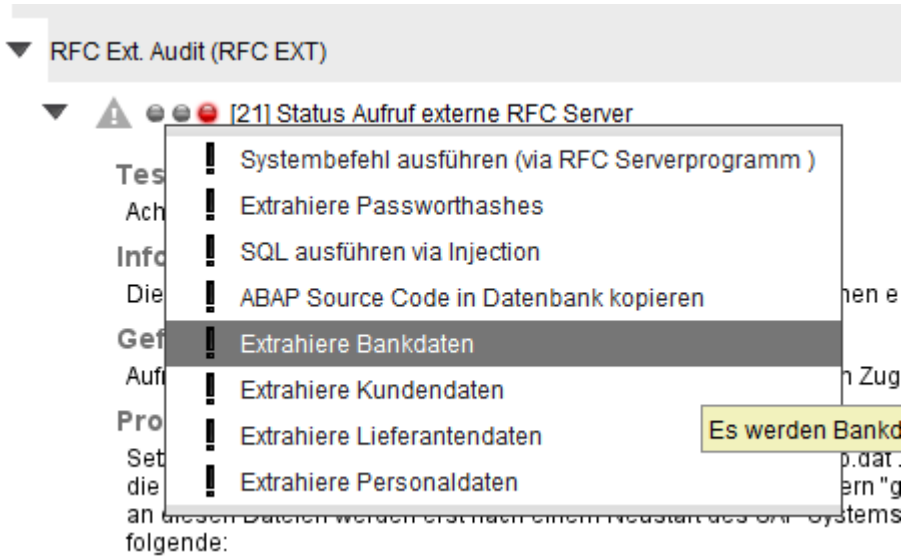


(Bild 2: Auszug aus der Liste der definierten Vertrauensstellungen im System)

Diese Verbindungen gewähren dem Angreifer von seinem aktuellen System aus Zugriff - ohne Abfrage weiterer Zugangsdaten. Dies macht sich der Angreifer zunutze, um Daten aus dem Produktivsystem auszulesen. Dazu ruft er die Transaktion SE37 auf und startet die Funktion RFC_READ_TABLE. Dort trägt er als Namen des RFC-Zielsystems den zuvor aufgespürten Namen der Trusted RFC-Verbindung ein (Bild 3).

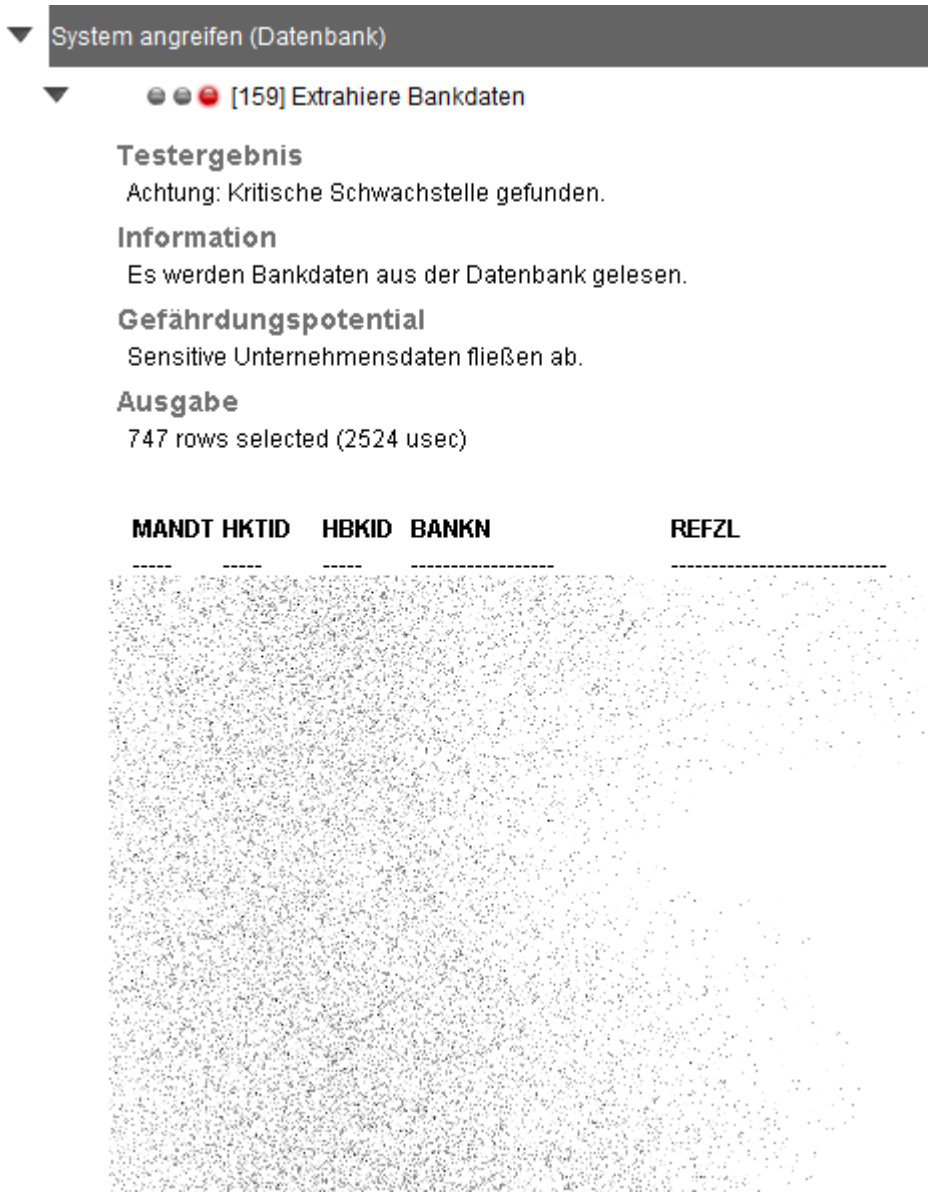
(Bild 3: Aufruf die Kundentabelle aus dem Produktivsystem auszulesen)
Startet er nun diesen Aufruf werden alle Kundendaten aus dem Produktivsystem angezeigt und der Datendiebstahl ist durchgeführt.

Alternativ hätte der Angreifer auch einen anderen Weg einschlagen können. Beispielsweise wenn die verschlüsselte Kommunikation mit SNC aktiv gewesen wäre. In diesem Fall wäre der Punkt 1 „unsichere Konfiguration des RFC-Gateways“ ein probates Mittel. Bei diesem Angriff benötigt der Angreifer keine Zugangsdaten um Befehle auf Betriebssystemebene abzusetzen und so unter anderem auf die Datenbank zu zugreifen. Bild 4 die identifizierte Schwachstelle in dem Produktivsystem und die Angriffsoptionen.



(Bild 4: Identifizierte Schwachstelle und Angriffsoptionen).

Das nachfolgende Bild 5 zeigt die Ergebnisse des erfolgreichen Angriffs und es konnten 747 Bankdatensätze ausgelesen werden.



(Bild 5: Ausgelesene Bankdaten)

Die Auswirkung von Cyberkriminalität

Die tatsächlichen Fälle von Wirtschaftsspionage, Datenmanipulation und -diebstahl durch Hacker-Angriffe sind schwer zu beziffern. Wenn ein solcher Angriff überhaupt entdeckt wird trifft er meist den Bereich Forschung und Entwicklung mit dem Ziel an Patentdaten zu gelangen oder Produkte nach zu ahmen.

Dies kann verheerende Folgen für das betroffene Unternehmen haben, wie eine Studie [4] von Ernst & Young zeigt: „*Plagiate treffen die deutsche Industrie ins Mark – schließlich ist der Standort Deutschland besonders auf Innovation angewiesen. Wenn Forschung und Entwicklung ins Leere laufen, weil Datendiebe die Gewinne einheimsen, wird das für die Wirtschaft im Land zum echten Problem.*" Das Schadenspotential ist jedoch weit vielfältiger. Ein Angriff auf das SAP-System kann zu einem kompletten Produktionsausfall führen, wenn das Herz der Firma für unbestimmte Zeit ausfällt. Ebenso können die gewonnen Daten aus dem HR-System gezielt zur Abwerbung der besten Mitarbeiter genutzt werden. Egal welcher Schaden eintritt, in der Regel folgt ein finanzieller Schaden entweder direkt oder indirekt. Den Vertrauensverlust beim Kunden gibt es dann oftmals gratis dazu.

Der Digitalverband Bitkom berechnet den Schaden für die gesamte deutsche Wirtschaft auf 51 Milliarden Euro pro Jahr [5]. Jedes Unternehmen muss für sich selbst in der Lage sein folgende Fragen beantworten zu können und daraus ableiten in welchem Maß Sicherheitsvorkehrungen notwendig sind:

- Wie viel Umsatz kann bei einem Datendiebstahl verloren gehen?
- Wie viel Umsatz kann durch die Folgen einer öffentlichen Berichterstattung entgehen?
- Wie viel Umsatz verliert man durch eine verringerte Produktivität durch einen Ausfall des SAP-Systems?
- Wie lange kann eine Untersuchung und Wiederherstellung des Systems dauern?
- Wie viel Geld könnte durch Strafzahlungen verloren gehen, weil vorgeschriebene Sicherheitsvorgaben nicht eingehalten wurden?

Sicher ist somit nur, dass Angreifer SAP-Systeme als lohnenswertes Ziel ausgemacht haben. Denn SAP-Systeme sind weit verbreitet und standardisiert. Mehr als 291.000 Kunden in 190 Ländern setzen SAP ein [8]. Sie produzieren 78% der weltweiten Lebensmittel und 82% der medizinischen Geräte. 74% der weltweiten Transaktionsumsätze durchlaufen SAP-Systeme. Eine Spezialisierung der Cyber-Kriminellen auf SAP-Systeme ist in vollem Gange.

Herausforderung Messung der SAP-Sicherheit

Wichtig für die realistische Sicherheitseinstufung der Systeme ist es die Grenzen der vorhandenen Schutzmaßnahmen und damit deren realen Nutzen zu kennen. So muss klar sein, dass Antivirus und Firewall moderne Trojaner nicht zu 100% abwehren können und ein Zugriff auf das Intranet für Angreifer möglich sein kann. Die Systeme im Intranet müssen also Robust sein und sich selbst gegen potentielle Angriffsversuche schützen können.
Ebenso sollte bekannt sein, dass hierzu das Berechtigungskonzept nicht ausreicht um SAP-Systeme zu schützen. Das Berechtigungskonzept wurde nie zur Abwehr von Cyber-Angriffen entwickelt.
Daher schützt es auch nicht vor:

- Fehlende Berechtigungsprüfungen in SAP
- Unzureichendes Logging (Security-Audit-Log Fehlkonfiguration)
- Potentiell gefährlicher Code in Custom ABAP Programmen
- technische Schwachstellen in SAP-Kern-Funktionen, dem Betriebssystem oder der Datenbank
- Sicherheitsrelevante Fehlkonfigurationen des Systems

Oftmals sind auch die Zuständigkeiten innerhalb einer Organisation nicht eindeutig geklärt und es fehlt die Abstimmung für den optimalen Schutz der Systeme. Nicht selten endet die Zuständigkeit des Security-Teams VOR dem SAP-System. Für die Sicherheit sind dann die SAP-Administratoren mehr oder weniger verantwortlich. Doch hier liegt oft das Augenmerk auf die Verfügbarkeit und Performance, denn auf die Sicherheit. Dies ist auch verständlich, da häufig das SAP-Team nur wenig Kenntnis von Hacker-Methoden, Exploits und Schadprogrammen besitzt. Auf der anderen Seite fehlt dem Security-Team die Kenntnis über die Besonderheiten und Konfiguration eines SAP-Systems.
Diese Herausforderungen gilt es zu meistern.

Sicherheit von SAP-Systemen realistisch bewerten

Wie kann man nun die Sicherheit der eigenen SAP-Systeme realistisch erfassen?

Der erste Schritt besteht in der Inventarisierung.
Ermitteln Sie Ihre geschäftskritischen SAP-Systeme. Klären Sie wer für die Systeme auf Prozess- und IT-Ebene verantwortlich ist. Insbesondere gilt es die Zuständigkeiten korrekt abzuklären. Letztlich sollten das SAP-Team und das Security-Team gemeinsam für die Sicherheit der Systeme sorgen. Das SAP-Team setzt die Maßnahmen um und das Security-Team kontrolliert die Wirksamkeit. So wird ein Schutz nach dem 4-Augen-Prinzip aufgebaut.

Im nächsten Schritt gilt es die existierenden Bedrohungen zu erfassen. Zur Erfassung der Systemschwachstellen von SAP-Systemen bietet sich der Einsatz entsprechender Werkzeuge, wie SAP-Security-Scanner, an. Damit die Bewertung und der Umfang solcher Werkzeuge in das rechte Licht gerückt werden kann, sollte man sich SAP-Security-Best-Praxis-Ansätzen (BSI-Grundschutz Dokumente zu SAP-Systemen, DSAG-Prüfleitfaden, SAP-Security-Guides) vertraut machen. So kann man bewerten ob alle relevanten Bereiche, Angriffswege und Sicherheitsmaßnahmen kontrolliert werden.

Weiter geht es mit der Bewertung. Dazu muss zunächst die Risikobereitschaft ermittelt werden. Da Risikomanagement eine Kernaufgabe der Geschäftsführung ist und nicht delegiert werden kann, ist nur diese Ihr Ansprechpartner um die gewünschte Risikobereitschaft zu besprechen. Sollte die noch nicht ermittelt worden sein, legen Sie mit der Geschäftsführung fest, welche Risikobereitschaft gewünscht ist. Idealerweise können Sie der Geschäftsführung hier bereits einen Vorschlag des angestrebten Sicherheitsniveaus unterbreiten und begründen, da die Geschäftsführung auf diesem Thema meist auf Führung angewiesen ist. Definieren Sie welche Risiken unbedingt zu mindern sind und halten fest warum.

Nachdem nun der Ist-Zustand und das gewünschte Risikolevel bekannt sind, gilt es die Abweichungen von Ist und Soll zu beseitigen.
Bestimmen Sie ein Team oder eine Person, die verantwortlich sein wird das definierte und akzeptierte Risikolevel zu erreichen und zu halten. Diese Aufgabe sollte das SAP-Basis Team übernehmen und entsprechend Ressourcen zur Bewältigung der Aufgaben erhalten. Hier ist der Rückhalt der Geschäftsführung erforderlich, damit Security-Aufgaben nicht Opfer anderer dringender Tätigkeiten werden. Dieser Punkt ist nicht zu unterschätzen, da das SAP-Team oft schon eine hohe Auslastung besitzt und gewisse Aufgaben der Sicherheit des Systems unterordnen muss.

Nun gilt es kontinuierlich den aktuellen Sicherheitslevel zu erfassen. Diese Aufgabe ist von dem Security-Team zu übernehmen. Da es oft schwierig ist überhaupt Experten auf diesem Gebiet zu finden oder diese nicht zu überlasten, sollte diese Aufgabe durch eine Automatisierung mittels Werkzeug unterstützt werden. Ein manuelles Abarbeiten der Best-Praxis-Dokumente wie DSAG-Prüfleitfaden oder SAP-Security-Guides ist vom Zeitaufwand nahezu nicht möglich. Aktueller Status, erforderliche Maßnahmen und der Verlauf des Sicherheitslevels muss durch das Werkzeug abgebildet werden. Auf diese Weise erkennt man sofort Handlungsnotwendigkeiten und kann den Fortschritt der umzusetzenden Maßnahmen überwachen.

Das richtige Werkzeug wählen

Bei der Auswahl eines Sicherheitsprogramms sind viele Aspekte zu beachten. Vornehmlich ist

jedoch Ihr Nutzen durch die Software zu beachten.
Grundlegend sollte die Prüfung der SAP-Systeme ohne Vorkenntnisse möglich sein. Spezielles SAP-Security Know-how darf keine Voraussetzung für die Nutzung sein, sondern muss durch die Software bereitgestellt werden. Ebenso ist eine intuitive Bedienung wünschenswert, die Bedienung des SAP-Systems ist doch bereits komplex genug. Die Installation und Einrichtung der Software sollte schnell von statten gehen und nicht zu einem eigenständigen mehrtätigen Projekt ausufern.
Besonders wichtig ist, dass die Software getrennt von dem zu prüfenden SAP-System läuft. Sie sollte nicht innerhalb dieser Systeme laufen, da dies zwangsläufig zu einer Änderung der eigentlich "nur" zu prüfenden Systeme führt. Damit wird der Prüfgegenstand durch die Prüfung geändert, dies ist unbedingt zu vermeiden.
Ein weiterer wichtiger Punkt bei der Auswahl ist die Qualität. Hier ist auf Qualität Made in Germany wie SAP selbst zu achten. Zuverlässige und reproduzierbare Ergebnisse sind ein Muss.
Der Prüfungsumfang der Software muss alle relevanten Bereiche abdecken. Die Software muss in der Lage sein die folgenden Aspekte zu prüfen:

- Prüfung der kritischen Berechtigungen und Berechtigungskombinationen
- Prüfung der System-Konfiguration
- Prüfung der SAP-Komponenten und -Schnittstellen auf technische Schwachstellen
- Prüfung des Custom ABAP-Programme
- Prüfung des aktuellen Patchstands
- Prüfung der System- und Security-Logs auf sicherheitskritische Ereignisse
- Prüfung des Betriebssystems und der Datenbank auf Schwachstellen

Positiv zu bewerten ist dabei eine Option zur automatischen Korrektur ermittelter Probleme. Verständliche Schritt für Schritt Anleitungen zur Problemlösungen sind zwingender Bestandteil einer solchen Security-Lösung.

Abschließend sind die Ausgaben der Software zu bewerten. Welche Berichtstypen werden angeboten und welche Formate werden unterstützt.
Berichte für das Management sowie für die technische Basis müssen elementarer Bestandteil sein. Zusätzlich sollten Maßnahmenpläne, Vergleichsübersichten und Berechtigungsmatrizen exportierbar sein. Dabei sind die gängigen Formate wie Excel, PDF, HTML zu unterstützen.
Letztlich sollte ein automatisierter Einsatz der Software möglich sein, um die knappen Ressourcen in einem Unternehmen optimal zu entlasten.

Zusammenfassung

SAP-Systeme besitzen einen hohen Stellenwert bei der Abwicklung der kritischen Geschäftsprozesse. Die hier gelagerten und verarbeiteten Daten sind sehr wertvoll. Verschiedenartig motivierte Angreifer haben den Wert der Systeme erkannt und verfügen über spezialisierte Angriffswege, um Zugriff auf die Systeme zu erhalten. Die Komplexität eines SAP-Systems ermöglicht mehrere Angriffsvarianten. Ein erfolgreicher Angriff hat immenses Schadenspotential für das betroffene Unternehmen. Zur Minimierung der Risiken muss eine kontinuierliche Überwachung des Sicherheitsniveaus der SAP-Systeme erfolgen und Maßnahmen zur Beseitigung von Schwachstellen abgeleitet und umgesetzt werden. Sicherheitsprogramme wie unsere Lösung Werth Auditor [1] unterstützen diesen Prozess und führen zu einer Entlastung der Ressourcen.

Quellen

[1] SAP-Security-Scanner Werth Auditor
http://www.werth-it.de

[2] SAP ERP System der Airports Authority of India (AAI) von Unbekannten lahmgelegt
http://blog.werth-it.de/blog/sap-erp-system-der-airports-authority-india-aai-von-unbekannten-lahmgelegt/

[3] China bestätig Existenz von Spezialeinheiten für den Cyber-War
http://blog.werth-it.de/blog/chinas-militaer-bestaetigt-offiziell-die-existenz-von-spezialeinheiten-fuer-den-cyber-war/

[4] EY Studie: Datenklau
http://www.ey.com/DE/de/Newsroom/News-releases/20130802-Datenklau---Neue-Herausforderungen-fuer-deutsche-Unternehmen

[5] Bitkom: Digitale Angriffe auf jedes 2. Unternehmen
https://www.bitkom.org/de/presse/8477_82074.aspx

[6] SAP-Security-Community
http://sapsecurity.werth-it.de/

[7] Cyberangriff via Hand-Scanner
http://blog.werth-it.de/blog/lager-scanner-spaehen-finanz-und-erp-daten-aus/

[8] SAP Factsheet
http://www.sap.com/bin/sapcom/de_de/downloadasset.2015-04-apr-21-01.SAP-Corporate-Fact-Sheet-de-20150421-pdf.bypassReg.html

[9] Hackerangriff auf deutschen Bundestag
https://www.tagesschau.de/inland/bundestag-hacker-angriff-101.html

[10] Antivirenhersteller ausspioniert
https://blog.kaspersky.com/kaspersky-statement-duqu-attack/

[11] Microsoft warnt vor Windows-Trojaner mit Angriffsziel SAP
http://blogs.technet.com/b/mmpc/archive/2013/11/20/carberp-based-trojan-attacking-sap.aspx

Über Werth IT

Die Werth IT GmbH kennt die Forderungen von Unternehmen an die IT-Sicherheit von SAP Systemen und nimmt den besonderen IT-Security-Bedarf sehr ernst. Aus diesem Grunde hat das Experten-Team mit hohem Bewusstsein für Qualität einen SAP-Security Scanner entwickelt, der vollständig das Prüfspektrum für SAP Systeme abdeckt.

Mit dem intuitiv bedienbaren SAP-Security Scanner setzt die Werth IT GmbH bewusst auf die leichte Handhabung und aussagekräftige Ergebnislisten, die heute bereits namhaften Unternehmen helfen, die vorhandenen SAP-Sicherheitslücken auch bei wachsender Komplexität und gleichzeitigem Fachkräftemangel effizient zu schließen.

Als Vorreiter in der IT-Security von SAP Systemen, ist es das Ziel der Werth IT GmbH das digitale Unternehmensdaten genau dort bleiben sollen, wo sie hingehören – nämlich im Unternehmen. Um das gemeinsam sicher zu erreichen, setzt sich der IT-Dienstleister voller Leidenschaft immer für faire Partnerschaften und wertschätzende Kundennähe ein.

WERTH

http://www.werth-it.de