Einleitung

SAP-Sicherheit ist in diesen Zeiten ein ganz naheliegendes Thema für ein Buch. Das Thema ist in den IT-Medien, aber auch in der Tagespresse und in den einschlägigen Internetforen allgegenwärtig. Das ist nicht verwunderlich, denn das Thema IT-Sicherheit hat spannende Komponenten, die auch für Laien interessant klingen. Ein Hack, d. h. ein Bruch der Sicherheit, bringt immer ein bisschen Nervenkitzel mit sich, und die dazugehörenden Technologien haben den Ruch des Gefährlichen und Bösen. Das Spiel mit Technologien, Computern, Software und den dadurch ermöglichten illegalen Tätigkeiten wird alljährlich in Las Vegas auf der Black Hat Convention zelebriert, auch wenn die dort präsentierten Vorgehensweisen und Techniken oft schon lange bei Sicherheitsexperten bekannt sind.

Sicherheit im SAP-Umfeld

Wie sollte aber nun ein Buch aussehen, das sich mit der professionellen Seite dieser Welt auseinandersetzt, den Sicherheitsfragen im Bereich großer SAP-Landschaften, den Bedürfnissen nach Angriffsabwehr und Grundschutz? In früheren Jahren sind die SAP-Systeme vor allem durch ihre Exklusivität geschützt worden, nicht zuletzt, weil diese meist in der dritten Ebene der Netzwerke lagen, geschützt von mehreren Firewalls. Wenn ein Hacker dort vorbeikam, scheiterte er an solch exotischen Technologien wie RFC-Gateways und SAP-Transaktionen. Solange die Webserver des Online-Handels schneller zu hacken waren, waren die SAP-Systeme weitgehend geschützt.

Das hat sich aber grundlegend gewandelt. Die Wirtschaftsspionage hat entdeckt, dass SAP-Systeme eine wahre Fundgrube sind. Die kriminellen Hacker haben entdeckt, dass man mit Schutzgelderpressung im SAP-Cyberspace gut weiter kommt. Und die Geheimdienste haben entdeckt, dass alles zusammen gute Informationen liefert.

Bei dieser gefährlichen Mischung aus finanzieller, krimineller und geopolitischer Herausforderung ist es offensichtlich, dass gerade die Kronjuwelen eines Unternehmens, die SAP-Systeme mit allen zentralen Unternehmensdaten, in den letzten Jahren in den Mittelpunkt von Hacks und kriminellen Cyber-Aktivitäten traten. SAP-Systeme, die vor allem aufgrund ihrer Größe, ihrer Komplexität und ihrer

Wichtigkeit in den Unternehmen schon immer eine besondere Rolle innerhalb der IT-Landschaft gespielt haben, verlangen nun auch im Bereich der Sicherheit eine spezielle Vorgehensweise.

Zielsetzung des Buches

In diesem Buch haben wir versucht, einen möglichst umfassenden Rundgang durch die wichtigsten Gebiete der SAP-Sicherheit zu machen. Es ist Ziel dieses Buches, Sie für die Bedrohungen in den SAP-Sicherheitsszenarien zu sensibilisieren. Kein Thema kann hier umfassend dargestellt werden, weshalb es die Idee der einzelnen Kapiteln ist, wichtige Inhalte zu skizzieren und Sie an den Stellen, die für Ihr Unternehmen wichtig erscheinen, selbst weiter arbeiten zu lassen. Das Buch soll in jedem Abschnitt Ihre Wahrnehmung für die Sicherheitsbelange schärfen. Sehen Sie sich anschließend die beschriebenen Themen in Ihren Projekten und Systemen in der Praxis an und entscheiden Sie selbst, welche Schlüsse Sie mit den zur Verfügung gestellten Informationen ziehen.

Wir haben beim Schreiben dieses Buches die goldene Regel respektiert, dass wir nur Sicherheitslücken beschreiben, für die es offiziell ein Gegenmittel, einen Schutz gibt. Falls Sie erwarten, in diesem Buch Beschreibungen von exklusiven Zero-Day-Exploits zu lesen, um SAP-Systeme einfach zu kompromittieren, werden Sie daher enttäuscht. Trotzdem werden Sie feststellen, dass es genügend spannende Themen zu entdecken gibt.

Wir können Ihnen mit diesem Buch keine vollständige Liste an Maßnahmen bereitstellen, die man abarbeiten muss, um das ultimativ sichere SAP-System zu erhalten. Es gibt kein universales Vorgehen für Sicherheit, und es gibt kein SAP-Modul, das man installieren kann, um fortan geschützt zu sein, wie teuer es auch sein möge. Sicherheit herzustellen ist, wie Sie bei der Lektüre dieses Buches erkennen werden, immer ein dauerndes, nie endendes Projekt, das immer wieder mit den aktuellen Ereignissen Schritt halten muss und immer wieder an die Spitze der Sicherheitsbemühungen vorauseilen muss.

Aufbau des Buches

Wir beginnen daher das Buch, indem wir in **Kapitel 1**, »Risiko- und Bedrohungsanalyse für SAP-Systeme«, allgemein die Risiken für SAP-Landschaften betrachten. Dabei geht es vor allem um die formalen Überlegungen, wie Sie Sicherheitsrisiken für Ihr System oder Ihr Projekt bewerten können, um auf der Basis einer sauberen Bewertung jeder einzelnen Risikokomponente (sei es nun SAP-Hardware,

SAP-Software oder ein einzelnes SAP-Modul) eine formale Bewertung vorzunehmen.

In **Kapitel 2**, »Eine Sicherheitsstrategie entwickeln«, sehen wir uns an konkreten Beispielen an, wie man eine solche Strategie für eine SAP-Landschaft im eigenen Unternehmen entwickeln kann. Dabei stellen wir mögliche Handlungswege für Unternehmen sowie Projekte und Sicherheitssysteme vor. Die wichtigste Erkenntnis ist, dass Sicherheit ohne fest definierte interne und externe Kommunikation und direkte Intervention nicht mehr gewährleistet werden kann. Ein deutsches Unternehmen hat ein nationales Sicherheitszentrum etabliert, in dem alle Sicherheitsfragen des Unternehmens zusammenlaufen. Dieses Projekt stellen wir als Fallbeispiel vor. Als zweites Beispiel dient uns ein *Wargame*, das das Bundesamt für Sicherheit in der Informationstechnik (BSI) durchgeführt hat, und das spannende Erkenntnisse über die Simulation von Angreifern und Verteidigern im Cyberspace bietet.

In **Kapitel 3**, »SAP-Sicherheit – Standards und aktuelle SAP-Werkzeuge«, stellen wir die Standard-Komponenten einer SAP-Landschaft vor, die abgesichert werden müssen. Zu ihrer Sicherung bieten einige SAP-Partner Werkzeuge an, die z. B. Angriffe automatisiert erkennen. Aber auch SAP selbst hat in den letzten Jahren nachgerüstet und eigene Werkzeuge auf den Markt gebracht, wie SAP Code Vulnerability Analysis zur Analyse von ABAP-Code und SAP Enterprise Threat Detection für die echtzeitnahe Überwachung der Systeme auf Basis der SAP-HANA-Technologie.

In **Kapitel 4**, »Netzwerksicherheit herstellen«, stellen wir die wichtigsten Netzwerkkomponenten und die Sicherheitsmaßnahmen vor, die zu ihrem Schutz möglich sind. Ziel dieser Darstellung ist es, einen Eindruck zu vermitteln, wie man durch eine Risikoabschätzung die Balance zwischen Kosten und Nutzen hält, ohne technisch die Kontrolle über das Netzwerk zu verlieren. In diesem Rahmen präsentieren wir auch das neue Konzept des Software-Defined Networking, das die Netzwerkadministration erleichtern soll und vor allem im Rahmen des Cloud Computings eine wichtige Rolle spielt. Technologien wie diese sind gerade dabei, die Sicherheitslandschaft von SAP-Systemen nachhaltig zu verändern.

In **Kapitel 5**, »Werkzeugkasten des SAP-Sicherheitsexperten«, werden die gängigsten Werkzeuge zur Netzwerkanalyse (auch *Hacker*

Tools genannt) vorgestellt. Wir konzentrieren uns hier auf die Kali-Distribution, die alle gängigen Hacker-Werkzeuge in einer Linux-Distribution vereinigt. Wir gehen explizit auf die doppelte Nutzung dieser Werkzeuge ein: Sowohl Angreifer (Black Hats) nutzen sie als auch die Sicherheitsexperten, die die Netzwerke mit Penetrationstests schützen wollen (White Hats).

In **Kapitel 6**, »Schutz von SAProuter und SAP Web Dispatcher«, beschreiben wir Angriffspunkte und Maßnahmen zum Schutze dieser wichtigen kritischen und vor allem zu sichernden Komponenten.

Kapitel 7, »Schutz des SAP NetWeaver AS ABAP«, beschreiben wir das technische Herzstück einer jeden SAP-Landschaft, den AS ABAP, die gängigsten Angriffsmuster auf den AS ABAP und die von SAP empfohlenen Maßnahmen zu seinem Schutz.

Kapitel 8 widmet sich dann dem SAP NetWeaver AS Java. In diesem Kapitel stellen wir das technische Herzstück für die Java-Komponenten einer SAP-Landschaft, die gängigsten Angriffsmuster auf den AS Java und die von SAP empfohlenen Maßnahmen zu seinem Schutz vor.

Kapitel 9, »Schutz von Remote Function Calls«, beschreibt die Funktionalität, den Angriff und den Schutz der zentralen Kommunikation der SAP-Systeme.

Kapitel 10, »Passwortschutz«, beschreibt die zentrale Problematik, die sich aus der Technologie der Passwörter in einer SAP-Landschaft ergibt. Wir analysieren Passwort-Policies, demonstrieren aber auch, wie man mit gängigen Werkzeugen diese Passwörter hacken kann. Die Art und Weise, wie vor allem ältere und ungenützte Passwörter im SAP-System gespeichert werden, ist immer wieder ein Problem. Deshalb zeigen wir in diesem Kapitel, wie die Angriffsvektoren (sogenannte *Hashes*) auf diese abgespeicherten Passwörter aussehen, welche Passwörter wie schnell entschlüsselt werden können und wie man dem begegnen kann.

Kapitel 11, »Schutz des Transportsystems«, betrachtet die technische Zentralkomponente zur Verwaltung von Transporten und Änderungsprozessen innerhalb einer SAP-Landschaft.

Der Schutz der Datenbank ist das Thema in **Kapitel 12**. Die Datenbank ist eines der kritischen Einfallstore für Angriffe, die von der

Netzwerkebene kommen. Da hier vor allem Sicherheitslücken der Datenbankhersteller genutzt werden, sind die Szenarien vielfältig. Wir untersuchen hier Angriffsmuster anhand von Fallbeispielen verschiedener Hersteller (IBM, Oracle, Microsoft).

Um die Datenbank SAP HANA geht es in **Kapitel 13,** »SAP HANA und die Sicherheit der In-Memory-Datenbanken«. SAP HANA ist ein neues Thema für die SAP-Sicherheit, das bisher kaum in den Bedrohungszenarien berücksichtigt wurde. Wir beleuchten hier vor allem den Aspekt der neuen Angriffe auf die Hauptspeicher der Systeme.

Kapitel 14, »Erkennung von Angriffsmustern und Forensik«, beschäftigt sich mit Logs, Forensik und SIEM-Systemen (Security Information and Event Management). Die Zukunft der Sicherheit in SAP-Systemen liegt nicht in besseren Firewalls oder Netzwerken. Sie liegt in der intelligenten Erkennung von technischen, sozialen und cyberbasierten Angriffen und deren Widerspiegelung in Netzwerkmustern. Dabei kommen viele Technologien (Netzwerkprotokolle, Behavioural Computing, Big Data, Echtzeit) zusammen. Eine neue Generation von Werkzeugen bedient sich dieser Technologien. Die Konzepte dieser Tools stellen wir in diesem Kapitel vor, gehen aber auch darauf ein, auf welche Daten und Logs die Forensik zugreifen kann, um Sicherheitsvorfälle aufzuklären.

Kapitel 15, »Mobile Anwendungen sichern«, beschreibt, wie man mobile Anwendungen sichern kann. Mobile Datenerfassung ist in Zukunft aus keinem Anwendungsfeld mehr wegzudenken. Wie sehen aber die Sicherheitskonzepte hierzu aus? Was muss alles beachtet werden, wenn man eine mobile Anwendung in ein SAP-Umfeld bringt? Diese Themen werden hier behandelt, zusammen mit dem Fokus auf der Sicherung der beteiligten Komponenten.

Das abschließende **Kapitel 16**, »Sicherheit im Internet der Dinge«, macht einen Ausflug in eine Welt, die SAP-Landschaften in Zukunft deutlich herausfordern wird. Das sogenannte *Internet der Dinge*, eine neue Generation von Anwendungen, spielt auch im SAP-Umfeld eine wichtige Rolle. Wenn per SAP RFC ganze Industrieanlagen gesteuert, bestückt und kontrolliert werden, wird diese Steuerung zu einem Sicherheitsrisiko. Auch die Welt der Hardwarehacks sprechen wir hier an und stellen einige Geräte vor, die ein Hacker oder Penetrationstester verwenden kann.

Nach der Lektüre sollten Sie als Leser einen guten Überblick über das Gebiet der SAP-Sicherheit, der SAP-Hardware, der SAP-Software und der Sicherheitssysteme für Ihre SAP-Landschaften haben. Von den Grundüberlegungen dieses Buches ausgehend sollten Sie dann Ihr eigenes Vorgehen in einem kleinen oder großen SAP-Security-Projekt ableiten können.

Umgang mit diesem Buch

In hervorgehobenen Informationskästen sind in diesem Buch Inhalte zu finden, die wissenswert und hilfreich sind, aber etwas außerhalb der eigentlichen Erläuterung stehen. Damit Sie die Informationen in den Kästen sofort einordnen können, haben wir die Kästen mit Symbolen gekennzeichnet:

[»] In Kästen, die mit diesem Symbol gekennzeichnet sind, finden Sie Informationen zu *weiterführenden Themen* oder wichtigen Inhalten, die Sie sich merken sollten.

[!] Dieses Symbol weist Sie auf *Besonderheiten* hin, *die Sie beachten sollten*. Es *warnt Sie* außerdem vor häufig gemachten Fehlern oder Problemen, die auftreten können.

[zB] *Beispiele*, durch dieses Symbol kenntlich gemacht, weisen auf Einsatzbeispiele aus der Praxis hin.

[+] Kästen mit diesem Icon geben Ihnen *Empfehlungen* zu Einstellungen oder *Tipps* aus der Berufspraxis.

Danksagung von Holger Stumm

Ein Buch zu schreiben, ist es ein großer Akt, und ich bin froh, dass ich auf Daniel Berlin, meinen Ko-Autor gestoßen bin, denn alleine wäre diese Buch nicht zu schaffen gewesen. Es ist die alte Projekt-Wahrheit, dass mehrere Köpfe auch mehr leisten, verschiedene Ansichten einbringen und dieser Dialog das Projekt vorwärts bringt.

Darüber hinaus möchte ich den SAP-Kollegen danken, die uns unterstützt haben, vor allem Dr. Jürgen Frank, Jürgen Adolf und natürlich Markus Ertel, der mir immer wieder weitergeholfen hat.

Des Weiteren danke ich Dr. Karl-Friedrich Thier von T-Systems für seine Hilfe bei dem Artikel über das Cyber Control Center und Thomas Werth von Werth-IT für seine Unterstützung und seinen Beitrag zu Kapitel 14, »Erkennung von Angriffsmustern und Forensik«.

Ralf Spenneberg von OpenSource Training danke ich für das spannende BSI-Training zu den Cyber-Attacken. Allen meinen Kolleginnen und Kollegen im Projekt der AXA Group Solutions in Köln sei gedankt, weil sie für alle meine Ideen und Ausführungen zur Security immer offen sind.

Und natürlich darf auch ein Dank an unsere geduldigen Lektorinnen beim Rheinwerk Verlag, Janina Schweitzer und Kerstin Billen, nicht fehlen.

Wer jemals Teil einer Familie war, in der ein Buch geschrieben wurde, weiß, was dies vor allem kurz vor Erreichen der Abschlusstermine bedeutet. Deshalb möchte ich mich ganz besonders bei meiner Frau Gisela bedanken, die mich auf diesem Weg immer begleitet und ermutigt hat. Django und Amelie möchte ich noch sagen, dass ich weiß, dass ich viel mehr Zeit haben müsste. Manchmal passieren in so einer Zeit auch tragische Dinge, und deshalb darf an dieser Stelle auch ein aus den Tiefen meiner Seele kommender Dank an meine Mutter Irmela nicht fehlen.

Danksagung von Daniel Berlin

Das Schreiben eines Buches ist einem IT-Projekt nicht unähnlich – nach der Planung, dem Kickoff und der ersten Phase des Schaffens stößt man auf Herausforderungen, richtet sich immer wieder neu aus und durchlebt Höhen und Tiefen. Ein gutes Team hilft hierbei enorm – ganz wie im gewohnten Projektgeschäft. In Holger Stumm habe ich einen besonnenen und fachlich herausragenden »Ko-Projektleiter« getroffen, ohne den unser Projekt nicht möglich gewesen wäre.

Darüber hinaus möchte ich Klaus Rettenmaier für seine unermüdlichen und stets hilfreichen Reviews danken, die er nicht nur im Rahmen dieses Buches durchgeführt hat.

Meinem Vater Volker Berlin danke ich für den C-64, der die lange Kette an Ereignissen ausgelöst hat, die letztlich zu diesem Buch führte, sowie für den schönen und interessanten Lebensweg bis hier und natürlich noch weiter.

Meinen Freunden Felix Taubert und Martina Kerstan danke ich für die Ermutigung und stetige Unterstützung in allen Lebenslagen. Ohne Euch wäre alles nur halb so schön.