

Hacking von SAP®-Systemen

Angriffe verstehen und abwehren

» Hier geht's
direkt
zum Buch

DAS VORWORT

Einleitung

2025 ist die Gegenwart unruhig, oder wie man neuerdings sagt, *volatil* geworden, und das Gleiche gilt auch für die Sicherheit. Es gibt eine Myriade von Unternehmen, die von der Sicherheitsberatung bis hin zu Sicherheitsprodukten alles anbieten, was die Unsicherheit von Unternehmen im Hinblick auf dieses Thema noch größer macht. Der Weltwirtschaftsgipfel in Davos verfasst jedes Jahr ein umfangreiches Cyber-Bulletin, das allen internationalen Führungskräften in den Flugkoffer gesteckt wird. Die Cloud als Herausforderung ist allgegenwärtig, und zusammen mit der Digitalisierung verlangt sie von Unternehmen eine Flexibilität und ein Innovationsdenken, wie es bisher nie gefordert war.

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

Das hat sich aber grundlegend geändert. Die Wirtschaftsspionage und die Hacker in der Cloud haben entdeckt, dass SAP-Systeme eine wahre Fundgrube sind. Kriminelle Hacker haben sich Schutzgelderpressung im SAP-Cyberspace zum Tagesgeschäft gemacht. Und die Geheimdienste haben entdeckt, dass SAP-Systeme viele gute Informationen liefern. Bei dieser gefährlichen Mischung aus finanziellen, kriminellen und geopolitischen Herausforderungen ist es offensichtlich, dass die Kronjuwelen eines Unternehmens, die SAP-Systeme mit allen zentralen Unternehmensdaten, in den letzten Jahren noch mehr in den Fokus von Hacks und kriminellen Cyberaktivitäten gerückt sind.

SAP-Systeme sind per se keine unsicheren Plattformen. Doch ihre enorme Komplexität, der oft über Jahrzehnte gewachsene Code und die Vielzahl an Schnittstellen machen sie zu einer Herausforderung für jede Sicherheitsstrategie. Noch problematischer ist der Umstand, dass Unternehmen häufig mit veralteten Konfigurationen, ungesicherten Berechtigungen oder fehlenden Updates arbeiten – ein gefundenes Fressen für Angreifer. Die wachsende Integration von Cloud-Technologien und hybriden Infrastruk-

Sicherheit in
SAP-Landschaften

Finanzielle,
kriminelle und
geopolitische
Herausforderungen

turen hat die Angriffsflächen weiter vergrößert, während gezielte Attacken raffinierter geworden sind.

**Zielsetzung
dieses Buches**

Und das spiegelt sich auch in unserem neuen Buch wider. Wir wollten hier nicht nur über Sicherheit sprechen, sondern die Hacks, Angriffe und die Möglichkeiten, SAP-Systeme und die SAP BTP zu hacken, auch realistisch darstellen. Aber was genau ist so gefährlich an den Bedrohungen aus dem Cyberspace, denen die Unternehmen angeblich ununterbrochen ausgesetzt sind? Können Sie dieses Risiko erfassen, beziffern und bewerten? Michael Hayden, ein ehemaliger General und Direktor der National Security Agency (NSA) der USA, hat dies bereits 2013 auf einer damals sehr beachteten Rede gegenüber Vorständen auf einem SAP-Kongress eindringlich formuliert:

»Sie müssen sich den Cyberspace als die neue Welt vorstellen. Denken Sie nicht in Bandbreite oder Kostenstellen – das Militär sieht es als realen Raum ... Wenn Sie nur etwas von Wert für uns haben, sind wir bereits bei Ihnen eingedrungen.«

Dieses Buch soll Ihnen einen fundierten Überblick über die wichtigsten Aspekte der SAP-Sicherheit geben. Unser Ziel ist es, Sie für die Bedrohungslage zu sensibilisieren und Ihnen praxisnahe Strategien aufzuzeigen, mit denen Sie Ihre SAP-Umgebung schützen können. Wir beleuchten nicht nur technische Maßnahmen, sondern auch organisatorische und prozessuale Aspekte, die für eine ganzheitliche Sicherheitsstrategie entscheidend sind.

Dabei verfolgen wir einen pragmatischen Ansatz: Es gibt keine Patentlösung für SAP-Sicherheit, keine einzelne Maßnahme, die ein System unangreifbar macht. Sicherheit ist ein kontinuierlicher Prozess, der sich an neue Bedrohungen anpassen muss. Deshalb beschreiben wir in diesem Buch keine Exploits, für die es keine offiziellen Gegenmaßnahmen gibt – unser Fokus liegt auf bewährten Methoden und praxisnahen Lösungen.

**Fortwährendes
Weiterbilden**

Dieses Buch soll Ihnen nicht nur Wissen vermitteln, sondern Sie auch zum Handeln anregen. Analysieren Sie Ihre eigenen SAP-Systeme, prüfen Sie bestehende Sicherheitskonzepte, und setzen Sie gezielt Maßnahmen um, die Ihr Unternehmen wirklich weiterbringen. Denn eines ist sicher: SAP-Sicherheit ist keine einmalige Aufgabe, sondern eine dauerhafte Herausforderung, die mit jeder neuen Technologie und jedem neuen Angriffsszenario weiterwächst.

Vor allem soll Sie dieses Buch neugierig machen. Sicherheit und Bedrohungen auch und gerade im SAP-Umfeld zu beobachten heißt, jeden Morgen aufs Neue gespannt zu sein, erfolgte Angriffe zu untersuchen und zu lernen. Trotzdem können wir in diesem Buch, so umfangreich es auch sein mag,

viele Themen und Produkte nur streifen. Stoßen Sie auf einen Begriff, der Ihnen interessant erscheint, oder auf einen Hacker-Ansatz, der Sie gespannt auf das Ergebnis macht: Recherchieren, lesen und lernen Sie weiter – das sollte Ihr Mantra sein.

Die Welt von Angriffen und Verteidigung in der IT, der Bedrohungen durch intelligente *Red Teams*, den Angreifern, und die geopolitische Verschmelzung mit Kriminalität in der Cyberwelt konstituieren sich immer wieder neu, werden immer komplexer und fordern deshalb immer mehr Wissen und Können in der Erkennung und Abwehr dieser Gefahren.

Auch die Künstliche Intelligenz (KI) ist inzwischen ein Werkzeug, das gerade in der Programmierung von Hacker-Werkzeugen und in der Analyse von Sicherheitsdaten häufig zum Einsatz kommt. Deshalb haben wir auch die KI, genauer ChatGPT um eine Stellungnahme zum Thema gebeten und folgende erhalten:

»Im digitalen Schattenreich ruhen weder Angreifer noch Verteidiger – mit jeder neuen Bedrohung wächst die Herausforderung, mit jedem Angriff die Notwendigkeit zur Wachsamkeit. Wer stehen bleibt, verliert, denn die Cyberwelt schläft nie.«

Wir beginnen daher das Buch, indem wir in **Kapitel 1**, Aktuelle Angriffsvektoren und Sicherheitsstrategien für SAP-Landschaften«, die aktuelle Bedrohungslage der letzten zwei Jahre zusammenfassen. Wir beschreiben die Hauptangriffsvektoren und klassische Lessons Learned aus Angriffen auf SAP-Anwenderunternehmen. Das Kapitel dient als Einführung in grundlegende Konzepte, um SAP-Sicherheit zu designen, aufzubauen und zu administrieren und die SAP-Systeme widerstandsfähiger zu machen und besser gegen digitale Angriffe abzusichern. Ziel ist es, den Blick zu weiten und von »sicheren Systemen« hin zu »resilienten Systemen«, also widerstandsfähigen SAP-Architekturen, zu kommen.

Aufbau des Buches

In **Kapitel 2**, »SAP-Sicherheit per Default: Standards und aktuelle SAP-Sicherheitswerkzeuge«, betrachten wir das Angebot von SAP im Bereich der Systemsicherheit. Es beginnt mit den grundlegenden Schutzmechanismen, die SAP bereits von Haus aus bietet. Dieses Kapitel gibt eine Übersicht über alle relevanten SAP-Produkte, die für den Schutz der Systeme entscheidend sind. Dabei werden sowohl klassische On-Premise-Lösungen als auch moderne Cloud-Sicherheitskonzepte betrachtet.

Bevor ein Angriff durchgeführt werden kann, muss ein Angreifer so viele Informationen wie möglich über das Zielsystem sammeln. Es stellt sich die Frage von **Kapitel 3**, »Wie kommen Hacker an die erforderlichen Informationen?«. In diesem Kapitel erläutern wir, wie Informationen zum Hacking

von SAP-Systemen durch eine einfache Google-Suche gesammelt werden können und wie mithilfe einer generativen KI wie ChatGPT Programme zur Unterstützung generiert werden können. Diese Methoden sind nicht nur für Angreifer, sondern auch für Sicherheitsverantwortliche von Interesse, um eigene Schwachstellen besser zu verstehen.

Jeder Handwerker braucht Werkzeuge – so auch Hacker. In **Kapitel 4**, »Was brauchen Hacker für On-Premise-Systeme? Ein Werkzeugkasten«, werden die Tools vorgestellt, die Hacker nutzen, um SAP-Systeme zu kompromittieren. Besonders im Fokus stehen Open-Source-Werkzeuge, die auf Plattformen wie GitHub frei verfügbar sind. Sicherheitsverantwortliche lernen, wie diese Tools funktionieren und welche Maßnahmen notwendig sind, um sich gegen solche Angriffe zu schützen.

In **Kapitel 5**, »Was brauchen Hacker für die SAP-Cloud? Mehr für den Werkzeugkasten«, gehen wir in die Cloud. Mit der zunehmenden Nutzung von Cloud-Technologien verändert sich auch die Art der Angriffe. Während On-Premise-Systeme oft mit spezialisierten SAP-Tools angegriffen werden, eröffnen sich in der Cloud völlig neue Möglichkeiten. Dieses Kapitel zeigt, wie Standard-Web-Hacking-Tools genutzt werden können, um SAP-Cloud-Systeme zu attackieren.

In **Kapitel 6**, »Erstes Ziel: das Netzwerk«, diskutieren wir, welche Sicherheitslücken das Netzwerkdesign von SAP-Kunden enthalten kann. Tatsächlich sind rund 70 % aller Unternehmen von Netzwerkschwachstellen betroffen, die von Angreifern gezielt ausgenutzt werden. Dieses Kapitel analysiert typische Fehler im Netzwerkdesign und erklärt, warum 90 % aller erfolgreichen SAP-Angriffe über diesen Vektor erfolgen.

In **Kapitel 7**, »Einmal im Netzwerk, werden die Passwörter gehackt: Passwortschutz«, zeigen wir, dass Passwörter nach wie vor ein kritischer Schwachpunkt sind. Anhand praxisnaher Beispiele erläutern wir gängige Methoden zur Kompromittierung von Passwörtern. Zudem zeigen wir, wie eine durchdachte Passwort-Policy und moderne Hash-Algorithmen zur Erhöhung der Sicherheit beitragen können – und warum die oft geforderte regelmäßige Passwortänderung eher kontraproduktiv ist.

Auch Standards können gefährlich sein. In **Kapitel 8**, »Welche SAP-Standardfunktionen können Hacker ausnutzen?«, werden Sie sehen, dass nicht jeder Angriff hoch entwickelte Tools erfordert. Oft sind es die Standardfunktionen von SAP, die ausgenutzt werden, um unautorisierten Zugriff auf Daten zu erlangen. In diesem Kapitel wird anhand von Beispielen gezeigt, wie sich ein Angreifer auch ohne spezielle Werkzeuge Zugang zu kritischen Daten und Funktionen in ABAP-Systemen verschaffen kann.

In **Kapitel 9**, »Angriff auf das SAP-System: Schutz von Remote Function Calls«, gehen wir auf einen klassischen, aber kritischen Angriffsvektor ein, den *Remote Function Call* (RFC). Dieses Kapitel beleuchtet, wie Angreifer diese Schnittstellen für unautorisierte Zugriffe nutzen und welche Schutzmechanismen Unternehmen implementieren können, um solche Attacken zu verhindern.

Um die eigenen Programme geht es in **Kapitel 10**, »Manipulation des kundeneigenen Codes: ABAP-Angriffe«. Denn Angriffe auf SAP-Systeme erfolgen nicht nur von außen – oft werden sie direkt im kundeneigenen Code ausgeführt. Dieses Kapitel zeigt, wie sich ABAP-Code manipulieren lässt und welche Sicherheitsmaßnahmen helfen, diese Risiken zu minimieren.

Daten sind das Ziel in **Kapitel 11**, »Angriffe auf SAP HANA und die In-Memory-Datenbank«. Die SAP-HANA-Datenbank ist das Herzstück vieler moderner SAP-Landschaften. Da sie jedoch eigene Sicherheitsmechanismen und spezifische Schwachstellen aufweist, ist es essenziell, sich mit ihrem Schutz auseinanderzusetzen. In diesem Kapitel werden typische Angriffsszenarien analysiert und entsprechende Schutzmaßnahmen vorgestellt.

In **Kapitel 12**, »Angriffe auf die SAP-Cloud-Infrastruktur«, sehen wir uns die SAP-Cloud-Systeme an, denn sie sind besonders anfällig für Angriffe auf Authentifizierungsmechanismen und APIs. Dieses Kapitel zeigt anhand praxisnaher Beispiele, wie Angriffe auf Microsoft Azure und SAP Business Technology Platform (SAP BTP) ablaufen und wie man sich dagegen wappnet.

Anwendungen in der Cloud sind Thema in **Kapitel 13**, »Angriffe auf SAP-Cloud-Anwendungen«. Hier wird der Fokus auf spezifische SAP-Cloud-Anwendungen gelegt, darunter SAP-Fiori-Anwendungen und die SAP Integration Suite. Sicherheitslücken in diesen Anwendungen können gravierende Auswirkungen haben, weshalb dieses Kapitel zeigt, wie solche Angriffe funktionieren und wie sie verhindert werden können.

Eine Ransomware-Erpressung im Detail zeigt **Kapitel 14**, »Ransomware: Ablauf eines Angriffs«. Hier wird ein komplettes Gesprächsprotokoll wiedergegeben. Sie können daran im Detail sehen, was passiert, wenn man mit den Erpressern einer Ransomware-Kampagne um Lösegeld feilscht und seine Daten zurückbekommen will. Das Kapitel gibt somit spannende Einblicke in eine dunkle Welt.

In **Kapitel 15**, »Berechtigungsbasierter Penetrationstest«, wird ein innovativer Ansatz vorgestellt, bei dem ein Prüfer in die Rolle eines Mitarbeiters mit umfassenden Rechten schlüpft. Der Test simuliert interne Bedrohungen und deckt Schwachstellen auf, die klassische Berechtigungsanalysen über-

sehen. Das Kapitel behandelt die technische Vorbereitung und Durchführung solcher Tests und fokussiert sich auf kritische Finanz- und Personaldaten, die besonders schützenswert sind.

In **Kapitel 16**, »Angriffe gegen mobile Anwendungen«, zeigen wir, dass mobile Geräte nicht nur ein fester Bestandteil vieler SAP-Cloud-Lösungen sind, sondern auch ein beliebtes Angriffsziel. Dieses Kapitel beleuchtet die spezifischen Bedrohungen für mobile Anwendungen und beschreibt Schutzmaßnahmen aus der Perspektive der mobilen Endgeräte.

In **Kapitel 17**, »Angriffe aus dem Internet der Dinge«, zeigen wir, dass es neben Software-Tools auch physische Geräte gibt, die Angreifer nutzen können. In diesem Kapitel werden einige der leistungsfähigsten und frei erhältlichen Gadgets vorgestellt, darunter Flipper Zero, der Shark Jack und das Pineapple. Diese Tools ermöglichen es, SAP-Systeme zu kompromittieren, Netzwerke zu analysieren und Schwachstellen auszunutzen.

Kapitel 18, »Härtung der SAP-S/4HANA-Plattform«, geht auf die Maßnahmen zur Härtung von SAP-S/4HANA-Systemen ein. Dazu gehören die richtigen Profileinstellungen im ABAP-Stack, Berechtigungskonzepte und der Schutz wichtiger Dateien auf Betriebssystemebene. Zudem erläutern wir, welche Reaktionsmöglichkeiten Unternehmen im Ernstfall haben, von der Sperrung einzelner Benutzer bis zur vollständigen Isolierung des Systems.

Kapitel 19, »Erkennung von Angriffen, Abwehr und Forensik«, befasst sich mit der Erkennung und Abwehr von Angriffen. Thread-Intelligence-Tools, SIEM-Systeme (Security Information Event Management) wie Microsoft Sentinel und Methoden zur forensischen Beweisaufnahme werden hier vorgestellt. Abschließend spielen wir ein Angriffsszenario durch, um zu zeigen, wie Unternehmen auf Bedrohungen reagieren können.

Informationskästen

In hervorgehobenen Informationskästen finden Sie in diesem Buch Inhalte, 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.



Die mit dem *Tippsymbol* gekennzeichneten Kästen geben Ihnen spezielle Empfehlungen, die Ihnen die Arbeit erleichtern können.



Kästen mit dem *Achtungssymbol* weisen Sie auf typische Probleme oder Fallstricke hin.

Praktische Beispiele zu den jeweiligen Themen sind mit diesem Symbol markiert.



Danksagung von Holger Stumm

Ein Buch zu schreiben ist es ein großer Akt, und ich bin froh, dass ich mit meinen Mitautoren Daniel Berlin, Thomas Tiede und Marcus Herold dieses Buch als Gemeinschaftswerk schaffen konnte. Wir kennen uns seit vielen Jahren aus gemeinsamen Projekten, und viele erinnern sich an die gemeinsamen »Hacker-Auftritte« von Thomas Tiede und mir auf Veranstaltungen wie der ICON in Hamburg. Es ist eine alte Projektweisheit, dass mehr Köpfe mehr leisten, verschiedene Ansichten einbringen und dass dieser Dialog das Projekt vorwärtsbringt.

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.

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

In diesen asymmetrischen Zeiten, in denen man sich jeden Tag mit Gefährdungen und internationalen Risiken beschäftigt, ist es oft wichtig, mindestens einmal am Tag den Kopf freizubekommen. Mein Umzug, beruflich wie privat, an das Stettiner Haff im äußersten Nordosten Deutschlands, an die Stelle, an der das Oder-Delta im Naturpark in die Ostsee fließt, ermöglichte ein tägliches Durchatmen im Lärm der Zeit. Hier kann man aus der Tür heraustreten und die Stille von Wald, Moor, Haff und Ostsee genießen. Deshalb soll dies auch eine kleine Danksagung an meine neue Heimat sein.

Danksagung von Daniel Berlin

Ein Buch zu schreiben ist kein Sprint, sondern ein Marathon – mit weniger Bewegung, aber genauso viel nötigem Durchhaltevermögen. Dieses Werk wäre nicht möglich gewesen ohne den großartigen Austausch mit meinen Mitautoren Holger Stumm, Thomas Tiede und Marcus Herold, mit denen ich über die Jahre hinweg viele spannende Diskussionen und gemeinsame Projekte erleben durfte. Mein Dank gilt auch dem Team des Rheinwerk Verlags, das unsere Gedanken in geordnete Bahnen gelenkt und das Buch mit scharfem Blick begleitet hat.

Ein besonderer Dank aber geht an meine Frau Yulia. Ohne ihre Unterstützung, ihr Verständnis und ihre Geduld wäre dieses Buch in dieser Form

nicht möglich gewesen. Sie hat mir den Raum gegeben, mich intensiv mit diesem Thema auseinanderzusetzen, und mich stets ermutigt, das Beste aus diesem Projekt zu machen. Dafür bin ich ihr unendlich dankbar.

Danksagung von Thomas Tiede

Seit vielen Jahren zeige ich in Vorträgen immer wieder, wie SAP-Systeme mit einfachsten Mitteln gehackt werden können. Dabei waren die Vorträge zusammen mit Holger Stumm besondere Highlights. An diesem Buch mitarbeiten zu dürfen war eine große Freude für mich. Daher gilt mein erster Dank meinen Mitautoren Holger Stumm, Daniel Berlin und Marcus Herold für die konstruktive Zusammenarbeit.

Vielen Dank auch an den Rheinwerk Verlag und insbesondere an unsere geduldige Lektorin Janina Schweitzer, mit der ich schon bei einigen Buchprojekten zusammenarbeiten durfte.

Darüber hinaus bedanke ich mich bei der IBS Schreiber GmbH, deren ABAP- und SAP-HANA-Systeme ich zum Testen und für Screenshots zu diesem Buch nutzen durfte.

Besonders bedanke ich mich bei meiner Frau Kristin für ihr Verständnis und ihre Geduld, insbesondere, da ich an zwei Buchprojekten parallel gearbeitet habe. Während dieser langen Schreibphase sind viele gemeinsame Aktivitäten ausgefallen, und sie hat sich zusätzlich intensiv um unseren Hund Thorin gekümmert, der in dieser Zeit zu uns kam. Dafür bin ich ihr sehr dankbar.

Danksagung von Marcus Herold

An diesem Buchprojekt mitwirken zu dürfen war für mich eine bereichernde Erfahrung. Der fachliche Austausch mit meinen erfahrenen Mitautoren Holger Stumm, Daniel Berlin und Thomas Tiede hat meine Perspektive erweitert und mir gezeigt, wie wertvoll kollaboratives Arbeiten sein kann.

Dem Team des Rheinwerk Verlags möchte ich für die professionelle Begleitung danken, die uns Autoren half, unsere Gedanken strukturiert zu Papier zu bringen.

Mein besonderer Dank gilt meiner Frau Annette, die mit ihrem Verständnis für meine eingeschränkte Freizeit dieses Projekt überhaupt erst ermöglicht hat. Und ohne die tatkräftige Unterstützung meiner Tochter Julica beim Korrekturlesen wäre mein Beitrag nicht in dieser Form zustande gekommen.