Compass Security Schweiz AG

Kurzbeschreibung & Projektablauf

Name des Dokuments:	compass_security_schweiz_ag_de.docx
Version:	v2.2
Datum:	31. Mai 2021
Klassifikation:	PUBLIC

Compass Security Schweiz AG, Werkstrasse 20, Postfach 2038, CH-8645 Jona
T +41 55 214 41 60, team.csch@compass-security.com, www.compass-security.com

Inhaltsverzeichnis

1 Kurzbeschreibung

Compass Security Schweiz AG ist ein auf Security Assessments und forensische Untersuchungen spezialisiertes Unternehmen mit Hauptsitz in Jona SG und Filialen in Bern, Zürich und Berlin, Deutschland. Im Auftrag des Kunden werden Penetrationstests und Security Reviews durchgeführt, um die IT-Sicherheit in Bezug auf Hacking-Attacken zu beurteilen sowie geeignete Massnahmen zur Verbesserung des Schutzes aufzuzeigen. Compass verfügt über grosse Erfahrung in nationalen und internationalen Projekten. Die enge Zusammenarbeit mit den Fachhochschulen Rapperswil und Luzern ermöglicht, angewandte Forschung zu betreiben, so dass die Compass-Sicherheitsspezialisten immer auf dem neusten Wissensstand sind.

1.1 Compass kurz und bündig

Gründungsjahr	1999
Gründer und Verwaltungsräte	Walter Sprenger, Ivan Bütler
Geschäftsführer Schweiz	Cyrill Brunschwiler
Firmensitz	Rapperswil-Jona SG, Schweiz
Filialen	Schweiz ▪ Zürich ▪ Bern Deutschland ▪ Berlin
Anzahl Mitarbeiter	55
Schwerpunkte	Angriffssimulation ▪ Ethical Hacking ▪ Penetration Testing ▪ Red Teaming ▪ Social Engineering Second Opinion ▪ Security Reviews ▪ Hardening Checks ▪ Technology Research Vorfallsbewältigung ▪ Incident Response ▪ Digitale Forensik Ausbildung ▪ Hands-on Training ▪ Awareness Vorträge ▪ Live Hackings
Projekte	600 Projekte pro Jahr ▪ 80% Angriffssimulation und Second Opinion ▪ 10% Digital Forensics und Incident Response ▪ 10% Trainings
Kunden	Finanzdienstleister, Pharma, Telekommunikation, Industrie, Energieversorgung, Schutz- und Rettungsorganisationen, Öffentliche Verwaltung, IT Dienstleister, Handel, Hi-Tech Startups etc.

1.2 Portfolio

1.2.1 Penetration Tests & Ethical Hacking

Beim Penetration Testing wird ein Angreifer simuliert, der unbefugt in einen Computer oder in ein Netzwerk eindringt. Damit erhält der Auftraggeber wichtige Hinweise, wo die Schwachstellen seines Systems oder seiner Organisation liegen und durch welche Massnahmen das Sicherheitsniveau verbessert werden kann. Dies wird auch als „Security Assessments“ bezeichnet und stellt die Kerndienstleistung der Compass Security dar.

1.2.2 Red Teaming

Red Teaming beschreibt eine vollständige, mehrstufige Simulation eines Angriffs auf ein Unternehmen. Das gesamte Red Teaming hat das Ziel, die Fähigkeit des Blue Teams zu trainieren und dessen Vorgehensweise zu beurteilen. Im Detail wird geprüft wie das Blue Team reale Angriffe erkennt, sich davor schützt und wie es reagiert. Im Vergleich zu einem traditionellen Penetrationstest finden Red Teaming Assessments oft über mehrere Wochen oder sogar Monate statt, um realistische Herangehensweise der Angreifer, des sogenannten Red Teams, zu ermöglichen.

1.2.3 Security Reviews & Audit

Bei Durchführung eines Security Reviews arbeitet Compass Security AG eng mit dem Kunden zusammen. Alle notwendigen Insiderdaten, Firewall-Konzepte oder System-Einstellungen werden offengelegt, um sich ein Bild über die Wirksamkeit von Schutzmassnahmen zu machen. Das Finden einer Sicherheitslücke im Source Code eines Programms ist aus Zeit- und Kostengründen oftmals effizienter als ein Penetration Test. Zudem können im Review-Verfahren auch Backend-Prozesse beurteilt werden. Security Reviews werden oftmals dort eingesetzt, wo neue Lösungen in Betrieb genommen werden und wo vor der produktiven Nutzung eine Gesamtaussage über die Verwundbarkeit gemacht werden soll. Ein Review wird als Entscheidungsgrundlage für die GO/No-GO-Meetings und Compliance Tests erstellt.

1.2.4 Forensic Services & Incident Handling

Die Computer-Forensik ist eine Methode zur Aufklärung von Computer-Delikten. Dabei werden digitale Spuren und mögliche Beweismittel erhoben, analysiert und dem Auftraggeber als Forensischer Bericht zur Verfügung gestellt. Damit erhält der Kunde wichtige Hinweise über einen Hacker-Einbruch und über die missbräuchliche Nutzung seiner Computer-Anlagen.

1.2.5 Security Training & E-Lab Courses

Nur wer aktuelle und zukünftige Angriffstechniken kennt, kann sich wirksam und längerfristig vor Hacker-Attacken schützen. In mehrtägigen Schulungen lernen die Kursteilnehmer die IT-Sicherheit von der praktischen Seite kennen und werden durch die Referenten der Compass Security sowohl in die theoretischen Prinzipien der Hacking-Verfahren als auch in die Abwehrmassnahmen eingeführt. Zu diesem Zweck hat Compass Security eine Hacking-Infrastruktur aufgebaut und entwickelt, die aus Laptops, eigens entwickelten Schulungsanwendungen sowie einer mobilen Server-Infrastruktur besteht. Damit werden die ISACA-Ausbildungen, Firmenkurse, Wargames und Hacking-Demos durchgeführt.

1.2.6 Compass-Produkte

Für den Austausch vertraulicher Unterlagen wie Offerten, Kundenunterlagen und Sicherheitsberichte hat Compass Security eine webbasierte Dokumentenablage mit dem Namen „FileBox“ entwickelt. Im Vergleich zu anderen Produkten liegt der Vorteil in der starken Authentisierung und der Einfachheit der Benutzung ohne vorherige Installation weiterer Software. Mehr Informationen unter: https://www.filebox-solution.com

Der Bereich E-Learning wurde ebenfalls zu einem Compass-Produkt ausgeweitet. In der interaktiven Hacking-Lab Infrastruktur können praktische Hacking-Fallbeispiele simuliert werden. Mehr Informationen unter: http://www.hacking-lab.com

Beide Produkte werden durch die Schwestergesellschaft "Compass Security Cyber Defense AG" entwickelt, vermarktet, vertrieben und betreut.

1.3 Warum Compass Security?

Compass Security wird von den Kunden aufgrund der hohen Kompetenz, Loyalität und Qualität der Ergebnisse gewählt. Die Mitarbeiter sind in der Lage, sowohl in der Sprache der Techniker, Projektleiter aber auch Geschäftsführer oder Verwaltungsräte zu sprechen und auf Augenhöhe die Bedeutung von Sicherheitslücken zu erläutern. Compass Security wird aufgrund der offenen Informationspolitik geschätzt. Die Tests werden dem Kunden transparent vermittelt. Compass Security ist auch an der Weitergabe und Schulung der Firmentechniker für die Sicherstellung einer langfristigen Security-Kontinuität interessiert. Die Verträge von Compass sind sehr kundenfreundlich. Sie sind ausgereift und auf den Schweizer und Europäischen Markt abgestimmt. Bedenken in Bezug auf IT-Ausfälle oder andere Probleme können mit dem Kunden besprochen und gelöst werden.

Jeder Auftrag ist individuell und auf die Bedürfnisse des Kunden zugeschnitten. Der Kunde erhält beim Offert-Meeting eine Beratung über die ideale Angebotsgestaltung, ohne dass Compass Security um jeden Preis die Dienstleistung verkaufen muss. Compass ist ehrlich im Umgang mit den Kunden. Falls Probleme auftauchen oder Fehler passiert sind, wird der Kunde umgehend informiert. Zudem ist Compass zuverlässig und pünktlich. Die abgemachten Zeiten und Termine werden eingehalten. Falls es zu Projektverzögerungen seitens Kunde kommt, ist Compass Security flexibel und kann aufgrund der internen Organisation darauf Rücksicht nehmen. All diese Aspekte zusammen sind für den Kunden eine USP (Unique Selling Proposition), was auch die langjährigen Kunden, die sich immer wieder durch Compass unterstützen lassen, beweisen.

1.3.1 Spezialisierung und Leistungsschwerpunkte

Eine Vielzahl der Compass Kunden sind risikobedingt vor allem in der Finanz- und Versicherungsbranche zu finden. Es gibt jedoch auch in anderen Branchen vermehrt ein erhöhtes Sicherheitsbedürfnis. Die umsatzreichsten Segmente sind nachfolgend aufgeführt:

- Internationale Banken, hauptsächlich mit Sitz in der Schweiz und Deutschland
- Private Banking in der Schweiz und Liechtenstein
- International aufgestellte Versicherungen
- Weltweite Industrie-, Pharma-, Chemie- und Logistik-Unternehmen
- Schweizer Telekommunikationsanbieter und -Lieferanten
- Schweizer Regierungsbehörden sowie kantonale und regionale Verwaltungen
- Schweizerische und Österreichische Betreiber kritischer Infrastrukturen
- Unternehmen, die in den "Fortune 500 " aufgeführt sind

Die Kundengrösse reicht von 10 bis 300'000 Mitarbeiter.

1.3.2 Mitarbeiter-Erfahrung und -Fähigkeiten

Compass-Mitarbeiter werden sehr sorgfältig ausgewählt und müssen einen eintragsfreien Strafregisterauszug nachweisen. Alle Teammitglieder haben einen Hochschulabschluss (Bachelor of Sciences, Bachelor in Engineering oder Master of Sciences) oder besitzen einen äquivalenten Leistungsausweis. Mitarbeitende werden in Compass-internen und einschlägigen externen Kursen geschult.

Die Compass Security Teammitglieder haben die folgenden Fähigkeiten und Erfahrungen (wobei sich einzelne auf ganz spezifische Themen spezialisiert haben, die hier nicht zusätzlich aufgeführt sind):

- Ein Mitarbeiter übernimmt rund 20 verschiedene Security-Projekte pro Jahr (hauptsächlich Penetrationstests und technische Reviews als auch die Analyse von Konzeptstudien).
- Alle Teammitglieder führen Infrastruktur-Assessments und Penetration Tests durch.
- Penetration Tester haben Kenntnisse über die OSSTMM (Open Source Security Testing Methodology Manual) und kennen Elemente aus den üblichen ISMS.
- Alle Teammitglieder führen Application Security Assessments durch.

- Teammitglieder halten Fachvorträge und erstellen Publikationen über VoIP, Skype und TLS-Sicherheit, über Phishing, Pharming und Trojaner, über Malware, mehrere Web-Applikations-spezifische Themen, Web 2.0 Sicherheitslücken, IPv6 Security, Wireless Security, DNS-Angriffe, Windows Exploiting usw., um nur einige zu nennen. Vollständige Liste auf https://compass-security.com/research/praesentationen/
- Teammitglieder veröffentlichen Advisories für Web-Anwendungen, Voice over IP-Lösungen (Nortel), Enterprise Resource Planning (SAP)-Tools sowie für Microsoft-Produkte, Citrix Terminal Server-Lösungen und den Linux-Kernel. Siehe https://compass-security.com/research/advisories/
- Compass Security ist Initiator der Swiss Cyber Storm Veranstaltung, eine internationale IT-Security-Konferenz mit Fachvorträgen und Wargame-Challenges, wo die Teilnehmer in einer Labumgebung Hacking Aufgaben lösen können. Siehe auch https://www.swisscyberstorm.com für weitere Informationen.
- Compass Security hat auf der bekannten Black Hat (Las Vegas) Konferenz bereits zweimal referiert.

2 Projektablauf

Compass Security legt hohen Wert auf eine enge Zusammenarbeit mit den Kunden. Nur dadurch kann in einem sensiblen Umfeld die Qualität der Resultate garantiert werden. Obwohl jedes Kundenprojekt spezifisch abgestimmt wird, folgt die Durchführung eines Projekts jeweils einem ähnlichen Muster. Dieses Vorgehen ist nachfolgend schematisch beschrieben.

2.1 Das Initialgespräch

Ein erstes Kundengespräch findet in der Regel telefonisch statt. Compass Security nimmt die Fragestellungen des Kunden auf und sondiert grob die Bedürfnisse des Kunden. Diese Phase eines Projekts wird meist durch ein Mitglied der Geschäftsleitung wahrgenommen. Ziel des Initialgesprächs ist die allenfalls notwendige Vorbereitung auf einen Termin für ein vertiefendes Beratungsgespräch, das bei Interesse vor Ort beim Kunden stattfindet.

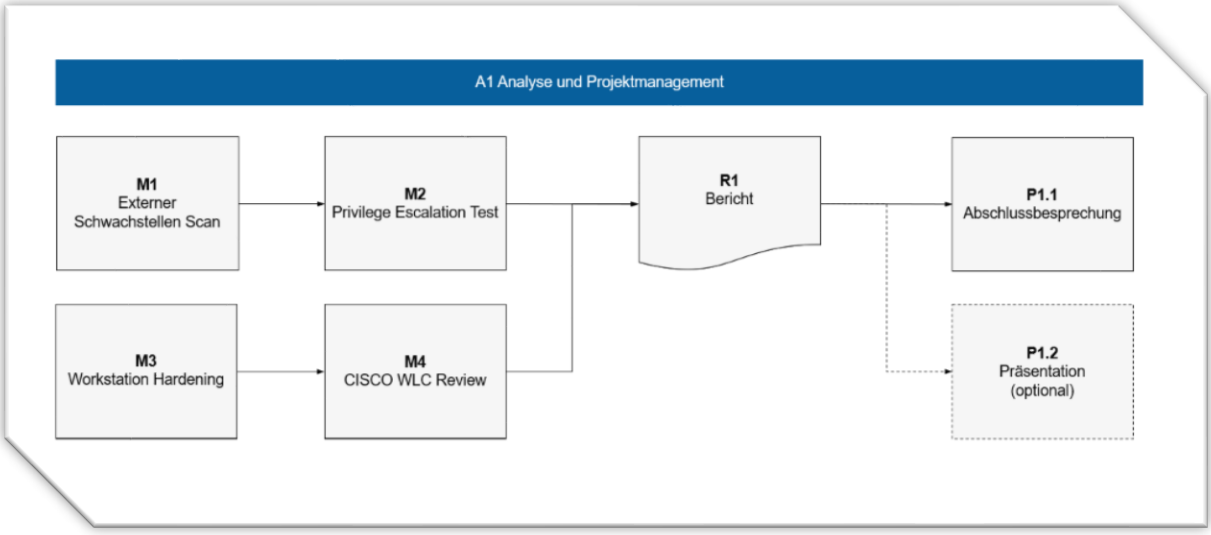
2.2 Die Besprechung

Im Rahmen eines Gesprächs, das immer von langjährigen Security-Analysten bzw. Mitgliedern der Geschäftsleitung durchgeführt wird, werden die Ideen, Fragen und Projektvorstellungen des Kunden detailliert besprochen und analysiert. Ziel ist es, die Bedürfnisse des Kunden zu verstehen und die modularen Bausteine typischer Testvorgehen auf den Kunden abzustimmen. Compass berät in diesem Zusammenhang auch über sinnvolle Projektergänzungen oder alternative und effizientere Methoden, nimmt terminliche Aspekte auf und definiert zusammen mit dem Kunden den Umfang des Projekts.

Gleichzeitig stellt Compass die eigene Arbeitsmethodik und -organisation vor, wie grundlegende Prinzipien der internen Projektrevision, dem Vier-Augen-Prinzip der Security-Analysten sowie bewährten Vorgehensweisen bei Abschlusspräsentationen resp. -besprechungen. Es wird auch die Form der Resultate, deren Struktur, Umfang und Aufbau aufgezeigt.

2.3 Das Angebot

Zum vereinbarten Termin erhält der Kunde die auf der Besprechung basierende Offerte. Sie bildet die Projektvorstellungen des Kunden in modularen Bausteinen ab. Diese Module sind eine bewährte Arbeitshilfe und erlauben es, auch komplexe Projekte sinnvoll zu gliedern und zu strukturieren. Jedes Modul dokumentiert dabei das Ziel einer Arbeit, die dazu notwendigen Voraussetzungen, sowie die geplante Vorgehensweise des Security-Analysten. Dem Kunden erlaubt die Aufstellung auch, die Aufwände für die Bereitstellung der notwendigen Dokumente, Unterlagen und Personalressourcen einzuschätzen.



Zudem werden in der Offerte die rechtlichen Rahmenbedingungen definiert. Beispielsweise ist es wichtig, alle vom Security Assessment betroffenen Parteien vorab zu involvieren. Dazu benötigt Compass, nebst der unterzeichneten Offerte, jeweils eine unterschriebene Einverständniserklärung aller involvierten Unternehmen.

Bereits in dieser Phase der Zusammenarbeit werden Compass-intern die benötigen Ressourcen zugeteilt und reserviert. Dadurch ist sichergestellt, dass bei Auftragseingang auch sofort die benötigten Ressourcen zur Verfügung stehen und termingerecht gearbeitet werden kann.

2.4 Die Projektvorbereitung

Der dem Projekt zugeteilte Compass-Projektleiter nimmt idealerweise vier Wochen, resp. spätestens zwei Wochen vor Projektbeginn Kontakt mit dem Kunden auf für die Vorbereitungen. Diese äusserst wichtige Phase des Projekts leitet das eigentliche Security Assessment ein. Dabei wird nochmals verifiziert, ob sich seit Offert-Stellung Änderungen im Projektfokus ergeben haben. Ausserdem wird der Security-Analyst alle für das Assessment notwendigen Detailabklärungen treffen, so dass das Projekt pünktlich und gemäss den tatsächlichen Kundenbedürfnissen durchgeführt werden kann. Unter anderem werden hier folgende Punkte definiert:

- Berichtsprache (deutsch, englisch, französisch, italienisch)
- Terminierung / Änderungen im zeitlichen Ablauf / Detailplanung
- Durchführungsort (Remote oder vor-Ort beim Kunden)
- Bestätigung der Ansprechpartner / technische Kontaktpersonen
- Beantwortung aller Fragen des Kunden zum Projektbeginn
- Abklären aller Voraussetzungen zum Projekt, z.B. Remote-Zugang, Vor-Ort-Badges usw.

Abschliessend vereinbaren Compass und Kunde zusammen einen definitiven Termin für den Projektstart, der in der Regel mit einem Kick-off-Meeting beginnt.

2.5 Der Projektbeginn

Das Kickoff-Meeting leitet das eigentliche Projekt beziehungsweise die Durchführung des Security Assessments ein. Der Compass-Projektleiter und zumeist auch alle weiteren, involvierten Analysten besprechen vor Ort die letzten zu klärenden Details, bevor mit den eigentlichen technischen Tests begonnen werden kann. Hier können auch sich kurzfristig ergebende Änderungen seitens des Kunden berücksichtig werden. Meist startet das Projekt dann noch am selben Tag. Das Kick-off-Meeting bietet dem Kunden auch die Möglichkeit, Rücksprache mit dem eigenen Team zu halten und wichtigen Punkten nochmals Gewicht zu verleihen. Ein Ziel ist dabei, dass alle Projektbeteiligten ein Gefühl für die Kommunikation und Arbeitsweise der Compass Security-Analysten bekommen und das Projekt möglichst effizient durchgeführt werden kann.

2.6 Die Projektdurchführung

Das Vorgehen während des eigentlichen Projekts ist natürlich stark von der Art des Auftrags abhängig und variiert dementsprechend stark. Gemeinsam ist jedoch allen Projekten, dass in enger Zusammenarbeit mit dem Kunden gearbeitet wird. Beispielsweise verschickt der Projektleiter täglich vor Beginn und nach Beendigung der Tests ein START- resp. STOPP-E-Mail an alle zuvor definierte Ansprechpartner des Kunden. Dadurch ist sichergestellt, dass der Kunde stets über die zu testenden Systeme auf dem Laufenden gehalten wird und sich intern darauf einstellen kann.

Auch während des Projekts können sich, beispielsweise aufgrund neuer Erkenntnisse, Änderungen im Projekt-Fokus ergeben. Der Compass-Projektleiter wird dann ad-hoc mit dem Kunden persönlich oder telefonisch Kontakt aufnehmen und abklären, ob und wie Compass die Arbeitsweise entsprechend anpassen soll. Das gleiche gilt für Aufträge, die weniger oder mehr Zeit als geplant in Anspruch nehmen. Compass reagiert in diesen Fällen professionell und flexibel.

Besonders gravierende Schwachstellen, die während des Projekts gefunden wurden, werden direkt und zeitnah an die zuvor vereinbarten Ansprechpartner kommuniziert. Dadurch ist sichergestellt, dass dem Kunden schwerwiegende Sicherheitslücken nicht bis zur Auslieferung des Berichts unbekannt bleiben, sondern direkt darauf reagiert werden kann. In diesen Fällen liefert Compass auf Anfrage gern Interims-Berichte, sogenannte DRAFTS, die spezifisch die entsprechenden Schwachstellen dokumentieren und erklären.

2.7 Der Abschlussbericht

Resultat eines jeden Projekts ist ein umfassender Bericht, der alle Sicherheitstest nachvollziehbar dokumentiert und in den Kontext zur Kunden-IT-Infrastruktur stellt. Anhand der eingearbeiteten Schwachstellentabelle ist der Kunde in der Lage, die identifizierten Sicherheitslücken gemäss der Compass-Bewertung einzuordnen und intern zu bewerten. Compass gewichtet dabei in vier Stufen:

INFO : zur Information
💣 : Gering
💣💣 : Mittel
💣💣💣 : Hoch

Die Gewichtung stellt KEINE Bewertung des Risikos oder der Eintretens-Wahrscheinlichkeit dar, da diese von kundenspezifischen Faktoren abhängig sind, die Compass Security nicht immer beurteilen kann. Das Compass-Rating ist daher rein technischer Natur und zeigt auf, wie einfach es für einen Angreifer ist, die beschriebene Schwachstelle auszunutzen.

Jeder Eintrag der Schwachstellentabelle referenziert den entsprechend dazugehörigen Test, so dass jeweils alle Details zu einer Sicherheitslücke verstanden und nachvollzogen werden können:

Nr.	Referenz	Schwachstelle	Bedrohung	Elimination	Wertung
1.	4.1 #2	**Cross-Site Scripting (XSS)** Benutzereingaben werden von der Applikation nicht kodiert, wenn diese an den Benutzer zurückgegeben werden.	Ein Angreifer hat die Möglichkeit, den Inhalt der Webseite im Browser des Benutzers zu manipulieren und etwa JavaScript Code in diese einzufügen. Aus Cross-Site Scripting resultierende Gefahren sind unter anderem: ▪ Stehlen der Benutzer-Session. ▪ Stehlen oder Manipulieren von Benutzerdaten ▪ Rechteausweitung, falls ein Administrator angegriffen werden kann. ▪ Umleiten eines Benutzers auf eine Phishing-Seite.	Wird ein Web-Framework für die Webseite eingesetzt, sollte die vom Framework zur Verfügung gestellte Funktionalität zur automatischen Enkodierung benutzt werden. Gefährliche Zeichen im Output müssen entsprechend den Regeln des jeweiligen Kontextes kodiert werden. Für regulären HTML Inhalt sollte HTML Kodierung verwendet werden: ▪ < -> < ▪ > -> > ▪ " -> " ▪ ' -> ' ▪ & -> &	
2.	4.8.2 #3	**Fehlendes Cookie-Flag: Secure** Die Session Cookie Einstellungen sind für eine durchgängig verschlüsselte Verbindung ungenügend. Das Secure Flag ist nicht gesetzt.	Die Cookie Einstellungen führen dazu, dass das Cookie auch über eine nicht verschlüsselte Verbindung gesendet wird.	Das Secure Flag sollte im Cookie gesetzt werden, sodass der Browser dieses nur über verschlüsselte Verbindungen versendet. Beispiel: `Set-Cookie: Cookie=Value; HttpOnly; Secure`	

Der Abschlussbericht wird in der Regel spätestens zwei Wochen nach Beendigung der Sicherheitstests ausgeliefert. Eine Vorab-Version des Berichts, der die interne Compass-Revision noch nicht durchlaufen hat, kann häufig direkt nach Testende zur Verfügung gestellt werden. So kann der Kunde diesen bereits prüfen und Compass mögliches Feedback geben. Zeitgleich kann der Kunde mit der Behebung von Schwachstellen in Zusammenarbeit mit den internen Experten beginnen.

Compass Security empfiehlt den Kunden, den Abschlussbericht intern zu diskutieren und jeder Schwachstelle eine eigene Risikobewertung zuzuordnen, um die Massnahmen entsprechend priorisieren zu können.

2.8 Die Abschluss-Besprechung und -Präsentation

Je nach Auftrag wird mit dem Kunden entweder eine Abschlussbesprechung oder eine Abschlusspräsentation vereinbart. Beide haben zum Ziel, den im Normalfall bereits zwei Wochen zuvor ausgelieferten Bericht zusammen zu diskutieren resp. der Projektleitung, der Fachabteilung oder dem Management verständlich zu erklären. Hier legt Compass vor allem Wert darauf, dem Kunden alle offenen Fragen und technischen Zusammenhänge nachvollziehbar darstellen und beantworten zu können.

Die Abschlussbesprechung bzw. Abschlusspräsentation markiert gleichzeitig das Ende eines Projekts. Es wird hier seitens der Compass sichergestellt, dass alle Bedürfnisse des Kunden erfüllt wurden. Compass steht natürlich auch im Nachgang, wenn das Projekt schon abgeschlossen ist, für Rückfragen zur Verfügung.