Vorwort

Lange Zeit hatte ich nicht vor, jemals ein Buch zum Thema Security zu schreiben. Ich sah meine Arbeitsschwerpunkte immer in der effektiven Bereitstellung von analytischen Systemen mit korrekten Daten, einer zweckmäßigen Architektur und einer Business-Intelligence-(BI-)Strategie, die sich wirklich an den Bedürfnissen des Business orientiert. Security war da nur eine ungeliebte Notwendigkeit.

Nachdem ich vor Jahren als Mitarbeiter in einem Business Intelligence Competence Center (BICC) eines internationalen Unternehmens mehrmals Berechtigungskonzepte definiert und implementiert hatte, wollte mich mein Chef zum Security-Officer für Business Intelligence machen. Ich sah mich eher als Datenmodellierer, Architekt und Projektleiter. Um diesem Job zu entgehen, ergriff ich ein lukratives Angebot und wechselte den Arbeitgeber, um wieder in der Rolle des Projektleiters arbeiten zu können.

Allerdings war ich auch bei diesem neuen Arbeitgeber mehrfach für die Erarbeitung von Security-Konzepten zuständig, sei es in Form von Berechtigungssystemen oder beim Design einer Architektur, die die geforderte Verfügbarkeit erfüllt.

Irgendwann musste ich mir eingestehen, dass Security einer der drei Teile der gesamten Qualitätssicherung einer BI-Plattform ist:

- Effektives Testen
- Datenqualität und Data Governance
- Security mit den Teilen Berechtigungen, Schutz vor Angreifern und angemessene Verfügbarkeit und Stabilität

Der Anstoß für dieses Buch kam schlussendlich während der Weiterentwicklung meines Seminars zum Testen von Data-Warehouse- und Business-Intelligence-Systemen. Ich war schon länger unzufrieden mit der Definition von Sicherheit in der ISO-Norm 9126[1], die Security nur als Teil der funktionalen Akzeptanzkriterien mit den Aspekten Zugriffsschutz auf Software und Daten bezeichnet. Eine

1. ISO 9126 definiert 23 Akzeptanzkriterien zur Prüfung der Ordnungsmäßigkeit eines Systems und ist somit Grundlage für die Definition messbarer Testfälle.

angemessene Verfügbarkeit, abhängig von einem vereinbarten Servicegrad, wird nicht berücksichtigt, ebenso wenig wie die Risikobetrachtung eines möglichen Angriffs und die Schaffung von Möglichkeiten zur Rückverfolgung. Bei der Erweiterung der Schulungsunterlagen um den Teil Penetrationstests wurde mir bewusst, wie umfassend das Thema war. Nach einem persönlichen Brainstorming meines Wissens zu Security reifte der Gedanke, dass daraus ein neues Buch entstehen könnte.

Definition und Instrumente zum vorher erwähnten Servicegrad liefert das IT-Governance-Modell ITIL[2]. Allerdings deckt ITIL in seinen 26 Prozessen auch nur Teile der Security-Anforderungen ab, was ich mir als zertifizierter ITIL-Experte irgendwann eingestehen musste. ITIL deckt alle Anforderungen an die Systemverfügbarkeit und Wiederherstellung sehr gut ab, jedoch nur noch genügend, wenn es um Autorisierung und Berechtigungskonzepte geht. Der Schutz vor Hackerangriffen und die Wahrnehmung der Daten als Wert fehlen komplett. Generell orientiert sich ITIL nur an Systemen und Funktionen und nicht an Daten. Leider liefert auch COBIT als weiteres IT-Governance-Modell ungenügende Informationen.

Bei all den vorher erwähnten Frameworks fehlt die Sicht auf analytische Systeme wie Data Warehouses. Nachdem ich die notwendigen Puzzleteile für eine vollständige Security-Betrachtung in mehreren Frameworks gefunden hatte, entstand nun der endgültige Entschluss, ein Buch für die Anforderungen der BI-Community zu schreiben.

Sobald über Security gesprochen wird, haben viele Personen automatisch ein Bild von einem Hacker vor ihrem geistigen Auge. Dieser Hacker sitzt stundenlang alleine in einem schlecht beleuchteten Raum vor seinem Computer und versucht in ein fremdes System einzudringen. Angetrieben wird er in hohem Maße von krimineller Energie, teilweise im Auftrag von weiteren dunklen Gestalten, die ihn bei Erfolg fürstlich belohnen. Zuerst vorneweg: Ich verbringe nicht meine ganze Zeit vor dem Computer und sehe auch keinen Anreiz darin, in andere Systeme einzudringen, um mir einen Vorteil zu verschaffen. Das heißt, ich sah mich bei meiner Arbeit in der Vergangenheit nicht als Hacker. Beim Schreiben des Buches wurde mir allerdings bewusst, in wie viele Systeme ich schon eingedrungen bin, nur um die Sicherheitslücken zu finden und zu schließen. In den meisten Fällen, und das ist das Erschreckende daran, genügen dazu gewöhnliche Mittel wie ein DOS-Prompt, ein Texteditor oder ein Browser. Nur in speziellen Fällen habe ich zusätzliche Tools eingesetzt wie Portscanner, User Activity Tracker oder Kameras. Rückblickend muss ich jedoch zugeben, dass ich wohl doch gewisse Hackeraktivitäten an den Tag gelegt habe, allerdings nie zu meinem persönlichen Vergnügen oder um finanzielle Vorteile zu erreichen.

2. ITIL – IT Infrastructure Library, ein service- und kundenorientiertes IT-Governance-Modell.

Wenn über Security gesprochen wird, entsteht manchmal ein übersteigertes Bedrohungsbild. Grundsätzlich ist es richtig, beim Thema Security eine Kultur des Misstrauens an den Tag zu legen. Allerdings empfehle ich einen pragmatischen Umgang damit, ähnlich wie mit Viren, Bazillen oder Krankheiten im Alltag. Beispielsweise gestalten sich Türgriffe meistens als komplette Ökosysteme von verschiedenen Viren und Bakterien. Trotzdem hat niemand die Befürchtung, den heutigen Tag nicht zu überleben, wenn er eine Türe öffnet. Für normal gesunde Menschen genügen schon ein paar einfache Sicherheitsmaßnahmen wie beispielsweise das Händewaschen, insbesondere vor dem Kochen oder Essen, um sich vor Ansteckungen zu schützen. Natürlich gibt es noch weitere mögliche Maßnahmen wie das vorherige Anziehen von Einmalhandschuhen aus Latex, das Einsprühen der Türgriffe mit Desinfektionsmitteln vor der Berührung oder der Einbau von sich selbstöffnenden Türen. Dass diese Maßnahmen im realen Leben übertrieben sind, ist jedem klar. So ist auch ein übertriebener Umgang mit IT-Sicherheitsmaßnahmen zu vermeiden.

Nun bleibt mir nichts anderes übrig, als Ihnen viel Spaß beim Lesen zu wünschen und viel Erfolg bei der Verbesserung der Sicherheit Ihrer Systeme.

Herbert Stauffer
Fislisbach, im Mai 2018