Cassini GreenLab:
D!NG - Integrierte Sicherheitsarchitektur

Whitepaper:
Sicherheit agil planen und umsetzen

Version: 1.0

Status: Final

Autoren: Dana Nitzsche,
Inna Maliucova

Stand: 23.08.2018

1. Ausgangslage und Lösungsansatz

Das Management von (Informations-)Sicherheit in Unternehmen ist und wird zunehmend komplexer. Die zu behandelnden Themen sind umfangreich, inhaltlich sehr unterschiedlich und müssen in der Regel abteilungs- und funktionsübergreifend behandelt werden.
Schon längst ist eine Abarbeitung mittels klassischem Projektmanagement ("Wasserfall") viel zu langsam und unflexibel. Erschwerend kommt hinzu, dass sich das Umfeld, in welchem Sicherheitsthemen gesteuert werden, geprägt ist von hoher Unsicherheit. Rahmenbedingung in Form von gesetzlichen Vorgaben und Regelungen (z.B. DSGVO) unterliegen immer wieder Änderungen. Technologien entwickeln sich rasant, künftige Sicherheitslücken, Sicherheitsvorfälle und Herausforderungen lassen sich kaum vorhersehen und schon gar nicht planen.

Wir glauben, dass die Verwendung agiler Methoden, insbesondere Scrum als allgemeines Rahmenwerk für agiles Projektmanagement geeignet ist, um einigen der genannten Herausforderungen zu begegnen und die Sicherheitsorganisation innerhalb der Unternehmen zukunftsfähig auszurichten. Denn agiles Projektmanagement beschleunigt die Abarbeitung einzelner Aufgaben innerhalb von Iterationen und erhöht die Reaktionsfähigkeit maßgeblich. Neue Anforderungen und Abweichungen vom Plan können schneller berücksichtigt und bearbeitet werden. Der Mensch und die Kommunikation stehen im Mittelpunkt und ermöglichen es, effizient und gleichzeitig kreativ zu arbeiten. Mitarbeiter unterschiedlichster Abteilungen arbeiten selbstorganisiert und eigenverantwortlich zusammen. Durch diese abteilungsübergreifende Vernetzung von Sicherheitsthemen sowie Bündelung von benötigtem Know-how, Organisation von Meetings und Arbeitsaufgaben in klar definierten Zeitabschnitten und einer positiven Fehlerkultur mit regelmäßigem Feedback werden Korrektur- und Ergänzungsbedarfe im Projekt, sowie Fehler deutlich schneller identifiziert und frühzeitig korrigiert.

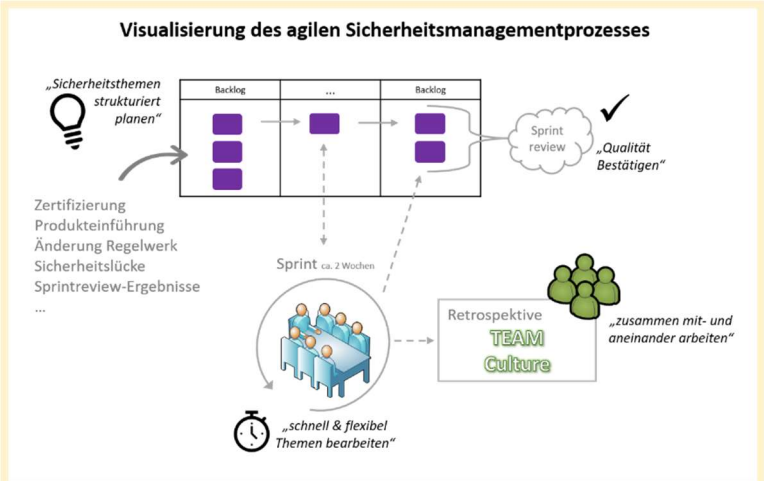
Nicht alle Bereiche innerhalb der Sicherheitsorganisation eines Unternehmens eignen sich für ein agiles Vorgehen. Zum Beispiel ist es im Rahmen vom Notfallmanagement oder bei der Bearbeitung von Sicherheitsvorfällen nicht möglich, Themen für eine Iteration (festgelegter Zeitraum) zu planen und dann in diesem Rahmen abzuarbeiten. Hier müssen die Mitarbeiter ad hoc reagieren. Nichtdestotrotz können bestimmte Elemente oder Methoden der agilen Vorgehensweise auch in diesem Bereich verwendet werden. Jede Organisation muss für sich definieren, in welchen Bereichen und in welcher konkreten Form agile Methoden (u.A. Scrum) angewendet werden.

2. Rollen und Teamzusammensetzung

Bei der Anwendung agiler Methoden zur schnellen Bearbeitung von Sicherheitsthemen müssen die klassischen aus dem agilen Umfeld bekannten Rollen ggfs. angepasst und erweitert werden. Jede Organisation muss individuell ihren eigenen Weg finden.
Kunde (oder Auftraggeber) ist immer die Unternehmensleitung, da dort auch die Gesamtverantwortung für die Sicherheit des Unternehmens liegt. Für einzelne Projekte/Vorhaben kann aber auch ein anderer interner oder externer Kunde definiert werden. Ebenfalls stellt sich die Frage, wie interdisziplinäre Teams zusammengestellt werden und ob es gegebenenfalls zusätzlich ein Kernteam für den Bereich Sicherheit geben muss.
Stakeholder, welche als Beobachter und Ratgeber beteiligt sind, gibt es definitiv immer. Die Stakeholder (Anwender, Manager) müssen aktiv gemanagt und auch inhaltlich mit einbezogen werden.

Scrum, als agile Methode aus der Softwareentwicklung stammend ist so allgemein beschrieben, dass es eher ein Rahmenwerk für agiles Prozessmanagement gesehene werden kann und relativ einfach auf andere Umfelder adaptiert werden kann. Aus unserer Sicht eignet sich Scrum demnach besonders um erste Schritte in Richtung eines agilen Managements von Sicherheitsthemen zu unternehmen.
Innerhalb dieses Rahmenwerks sind drei am Prozess beteiligte Rollen definiert.

1. Der **Product Owner**: vertritt die Interessen des Kunden gegenüber dem Scrum Team, stellt anhand der strategischen Zielsetzung fachlich Anforderungen welche als User Stories formuliert sind und priorisiert diese. Aus unserer Sicht muss der Product Owner für die Sicherheitsorganisation zusätzlich sicherstellen, dass die Anforderungen der bestehenden Regelwerke in Bezug auf Sicherheit (VSA, DSGVO…) auf das Unternehmen angepasst, heruntergebrochen und spezifiziert werden und dann natürlich auch in die Umsetzung gehen.
2. Der **Scrum Master**: managt den Scrum Prozess und beseitigt Hindernisse. In der Regel fungiert er als Coach und Berater für das Scrum Team. Wir sehen auch hier ein erweitertes Kompetenzprofil, in dem er operativer in den Sprintaktivitäten beteiligt ist und eine fachliche Führungsrolle übernimmt. Geeignet für diese Position sind die Security Officer (SO), welche per se schon eine Querschnittsfunktion in ihren jeweiligen Fachbereichen wahrnehmen.
3. Das **Scrum Team**: setzt die einzelnen Tasks um. Im Endeffekt wird es für die Sicherheitsorganisation eines Unternehmens mehrere agile Teams geben, die an unterschiedlichen Inhalten arbeiten (z.B. Zertifizierung, Einführung neuer Verfahren, Beschäftigung mit Technologieneuerung). Hierbei muss die Zusammenstellung projekt- und themenspezifisch unter Berücksichtigung der jeweils benötigten fachlichen und technischen Expertise erfolgen. Je nach Unternehmensgröße und Komplexität kann die Teamgröße variieren (5-7 Mitglieder). Das Srum Team muss in der Lage sein, die Tasks eigenständig und selbstorganisiert abzuarbeiten.



3. Anwendungsbeispiel

Anhand folgendem Szenario werden wir veranschaulichen, wie die Umsetzung von Sicherheitsanforderungen mittels agiler Methoden aussehen könnte.

- Ein Unternehmen möchte eine ISO27001 Zertifizierung auf Basis von IT-Grundschutz für sein Rechenzentrum nebst Dokumentenmanagementsystem.
- Das Projekt wird agil umgesetzt.
- Kunde des Projektes ist die Unternehmensleitung, Product Owner ist der Informationssicherheitsbeauftragte (InfSiBe). Er benennt als Scrum Master den SO (Security Officer) des Rechenzentrumsbetriebes. Dieser ist für seinen Bereich für die Planung und Koordinierung der Sicherheitsaktivitäten zuständig.

Schritt 1: Die Teamzusammenstellung

Wichtig: Alle relevanten fachlichen und technischen Kenntnisse müssen interdisziplinär vertreten sein. Für den Anfang wird ein 5-köpfiges Team gebildet, bestehend aus einem Mitarbeiter der Liegenschaftsinfrastruktur, einem Mitarbeiter Rechenzentrumsbetrieb, einem Mitarbeiter Rechenzentrumsplanung, einem Mitarbeiter aus dem Personalbereich sowie ein Experte für Risikomanagement.

Schritt 2: Sprintvorbereitung

Der InfSiBe definiert in seiner Rolle als Product Owner den IT-Verbund und die anzuwendenden Bausteine. Die Gesamtheit der zertifizierungsrelevanten Themen dieser Bausteine werden in User Stories umgewandelt und im Gesamt-Backlog zusammengefasst. In diesem Beispiel werden die User Stories direkt aus den Zertifizierungsanforderungen heraus definiert. Anhand der integrierten Testfälle („Definition of Done“) je User Story prüft der InfSiBe dann die erfolgreiche Umsetzung.
Anschließend werden die einzelnen User Stories priorisiert. Ergebnis ist eine eindeutige, nummerisch geordnete Liste, die in der Verantwortlichkeit des Product Owners liegt.
Im Sprint Planning wird eine erste umzusetzende Teilmenge festgelegt. Hierfür werden die am höchsten priorisierten Stories ausgewählt und durch das Team gemeinsam mit Story Points versehen ("agile estimation"). Das Team bricht nun jede einzelne User Storie in konkrete Tasks runter.
Im Ergebnis des ersten Sprint Plannings will das Team folgende User Stories umsetzen. Diese sind im Sprint Backlog dokumentiert:

User Stories und Tasks (Auszug):

a. Als Facility Mgmt muss ein Zutrittskonzept vorliegen, um Zutritt nur auf berechtigte Mitarbeiter einschränken zu können.
b. Als Planer muss ich eine digitale Übersicht über die Rack-Belegung im Rechenzentrum haben, um Wartungsarbeiten sicher durchzuführen zu können.
c. Als InfSiBe muss ich eine formale Anmeldung zur Zertifizierung senden, um den Zertifikatsprozess zu starten.

AGILES GLOSSAR

User Stories = umzusetzende "Kunden"-Anforderung, welche nach einem vordefinierten Muster aus Sicht des Kunden inkl. Nutzem erstellt wird. In unserem Fall Vorgabe/Maßnahme aus dem Regelwerk IT-Grundschutz.
Gesamt-Backlog ("Product-Backlog") = Gesamtheit aller User Stories, wird fortlaufend ergänzt und modifiziert (neue Stories kommen hinzu, andere werden entfernt oder modifiziert)
Definition of Done = gemeinsames Verständnis des Teams, wann etwas fertig gestellt ist (z.B. Tests, Freigabe)
Agile estimation = Schätzung der Umsetzung der einzelnen Kundenanforderungen. In der Regel werden Aufwand ("wie groß ist die umzusetzende Anforderung" anhand z.B. Story Points oder T-Shirt sizes) und Geschwindigkeit ("wie lange dauert es, bis eine Anforderung umgesetzt wird" z.B. mittels velocity Data).
Task = konkrete Aufgabe die im Sprint umgesetzt wird
Sprint Backlog = Auswahl der in diesem Sprint umzusetzenden Tasks, welche die ausgewählten User Stories herunterbrechen, nicht veränderbar

d. Als Anwendungs-Administrator muss ich Prozesse für Identitäts- und Berechtigungsmanagement definieren, um Zugriffe restriktiv steuern zu können.
   i. Für diese User Story werden 4 Task definiert:
      1. Eine Policy zur Einrichtung von Benutzergruppen verfassen.
      2. Prozess zur Identitätsprüfung erstellen
      3. Passwortgebrauch regeln
      4. Verfahren zum Zurücksetzen von Passwörtern definieren

Es wird eine Sprintdauer von 2 Wochen festgelegt, in der das Team insgesamt 20 Task abarbeiten möchte. Das Team arbeitet selbstorganisiert und jedes Teammitglied wählt seine Tasks selbstständig aus.

Schritt 3: Der Sprint

Der Fortschritt der einzelnen Tasks wird am Taskboard visualisiert. Dieses nimmt eine ganze Wand vor dem Projektraum ein. So wissen alle Teammitglieder und auch Product Owner und Projektstakeholder, wo das Projekt gerade steht und welchen Inhalten gearbeitet wird.
Jeden Morgen tauscht sich das Team im Daily aus. Der Scrum Master nimmt sich im Nachgang der aufgekommenen Hindernisse (möglicher Hindernisse) an und stellt sicher, dass alle Teammitglieder ungestört an ihren Tasks arbeiten können.
Bei nicht-technischen Tasks ist die Reihenfolge der Abarbeitung nicht ganz so relevant. Als Ergebnis stehen am Ende des Sprints ein beziehungsweise in diesem Fall mehrere Inkremente. Die fertige Policy zur Einrichtung von Benutzergruppen im Dokumentenmanagementsystems, das bereits verwendbare Template zur Berechtigungsanmeldung, sowie eine Checkliste zur Zutrittsanmeldung wird gegen die im Vorfeld festgelegte Definition of Done gegengeprüft.

Schritt 4: Das Sprint Review

Nach dem zweiwöchigen Sprint kommt das Team und alle Stakeholder zum 2-stündigen Sprint review ("timeboxed", je Sprint-Woche 1 Stunde) zusammen. Dort werden die fertigen Inkremente des Sprints präsentiert und auf vollständige Umsetzung hin geprüft. Bei dem Prozess zum Identitäts- und Berechtigungsmanagement fehlt ein Vorgehen beim Ausscheiden von Administratoren. Der InfSiBe formuliert daraufhin eine neue User Story, die in das Gesamt-Backlog aufgenommen wird. Neben Product Owner (hier der InfSiBe) geben auch weitere Stakeholder, zum Beispiel der Datenschutzbeauftragte Feedback, welches im nächsten Sprint berücksichtigt wird.

Schritt 5: Retrospektive

Der SO des Rechenzentrums, welcher Scrum Master ist, führt zum Abschluss mit dem Team eine Retrospektive durch. Das Team stellt fest, dass die Anzahl der User Stories so groß geworden ist, dass die bisher verwendete Excel-Tabelle nicht mehr ausreicht. Es wird über die Einfüh-

AGILES GLOSSAR

Daily = Stand-up und timeboxed (15min) Meeting in dem täglich von jedem Teammitglied 3 Fragen beantwortet werden: was habe ich gemacht, was werde ich heute tun und was hindert mich daran.
Inkrement = Ergebnis eines abgeschlossenen Tasks. Dieses muss aus einem vollständig fertig und potentiell produktiv einsetzbarem Anwendungsteil bestehen.
Timebox = grundlegendes Konzept im Scrum und maßgeblich zur Effizienzsteigerung. Meetings und Inkremente werden in einer festgelegten Zeitspanne abgehalten, welche nicht überschritten werden darf.
Retrospektive = Eine Diskussion über den eigentlichen Arbeitsprozess und die Zusammenarbeit des Teams während des Sprint. Das Ziel ist die kontinuierliche Verbesserung des Team-Zusammenspiels und damit der Produktivität des Teams.

rung eines Tools nachgedacht. Außerdem bemängeln einige Teammitglieder, dass ihre Tasks länger als ein Tag dauern und somit im Daily nicht viel bzw. gar nichts Neues berichtet wird. Man einigt sich auf einen 2-Tages-Rhythmus.

Schritt 6:…. weiter geht es zum nächsten Sprint.
In unserem Beispiel ist das fertige Produkt am Ende von x Sprints die erfolgreiche Zertifizierung.

Natürlich ist die Behandlung von Sicherheitsthemen innerhalb von Organisationen niemals abgeschlossen, sondern beinhaltet die fortlaufende Verbesserung und Weiterentwicklung der bereits etablierten Maßnahmen sowie die Reaktion und Aktion in Bezug auf sich ändernde Rahmenbedingungen aus dem externen und internen Umfeld, Umgang mit neuen Technologien, sowie mögliche und tatsächliche Sicherheitslücken.