Projekt Erfahrung Dr. Bernhard Bowitz, Dipl. Ing. CISSP, BSI 100

Das Grundprinzip eines SIEM-Systems ist, dass relevante Daten über die Sicherheit eines Unternehmens an mehreren Standorten produziert werden und in der Lage ist, alle Daten aus einer einzigen Sichtweise zu betrachten, macht es einfacher, Trends zu erkennen und Muster zu sehen, die außergewöhnlich sind . SIEM kombiniert SIM (Sicherheitsinformationsmanagement) und SEM (Security Event Management) in einem Sicherheitsmanagementsystem.

Ein SEM-System zentralisiert die Speicherung und Interpretation von Protokollen und ermöglicht eine Echtzeit-Analyse, die es dem Sicherheitspersonal ermöglicht, defensive Aktionen schneller zu machen. Ein SIM-System sammelt Daten in ein zentrales Repository für Trendanalyse und stellt automatisiertes Reporting für Compliance und zentrales Reporting zur Verfügung. Durch die Zusammenführung dieser beiden Funktionen bieten SIEM-Systeme eine schnellere Identifikation, Analyse und Wiederherstellung von Sicherheitsereignissen. Sie erlauben auch Compliance-Managern zu bestätigen, dass sie die gesetzlichen Anforderungen der Organisation erfüllen. (SCRUM* Vorgehen)

Ein SIEM-System sammelt Protokolle und andere sicherheitsrelevante Dokumentation für die Analyse. Die meisten SIEM-Systeme arbeiten, indem sie mehrere Sammelagenten hierarchisch einsetzen, um sicherheitsrelevante Ereignisse von Endbenutzergeräten, Servern, Netzwerkgeräten und sogar spezialisierten Sicherheitsausrüstungen wie Firewalls, Antivirus- oder Intrusion Prevention-Systemen zu sammeln. Die Sammler führen Ereignisse zu einer zentralen Management-Konsole, die Inspektionen und Flaggen Anomalien führt. Damit das System anomale Ereignisse identifizieren kann, ist es wichtig, dass der SIEM-Administrator zunächst unter normalen Ereignisbedingungen ein Profil des Systems erstellt.

*Scrum kennt drei Rollen für direkt am Prozeß Beteiligte: Product Owner (stellt fachliche Anforderungen und priorisiert sie), ScrumMaster (managed den Prozeß und beseitigt Hindernisse) und Team (entwickelt oder bearbeite das Produkt). Daneben gibt es als Beobachter und Ratgeber noch die Stakeholders.

Die Anforderungen (Requirements) werden in einer Liste (Product Backlog) gepflegt, erweitert und priorisiert. Das Product Backlog ist ständig im Fluß. Um ein sinnvolles Arbeiten zu ermöglichen, wird monatlich vom Team in Kooperation mit dem Product Owner ein definiertes Arbeitspaket dem oberen, höher priorisierten Ende des Product Backlogs entnommen und komplett in Funktionalität umgesetzt (inkl. Test und notwendiger Dokumentation). Dieses Arbeitspaket, das Increment, wird während der laufenden Iteration, des sog. Sprints, nicht durch Zusatzanforderungen modifiziert, um seine Fertigstellung nicht zu gefährden. Alle anderen Teile des Product Backlogs können vom Product Owner in Vorbereitung für den nachfolgenden Sprint verändert bzw. neu priorisiert werden

Das oder die Arbeitspaket/e wird/werden in kleinere Arbeitspakete (Tasks) heruntergebrochen und mit jeweils zuständigem Bearbeiter und täglich aktualisiertem Restaufwand in einer weiteren Liste, dem Sprint Backlog, festgehalten. Während des Sprints arbeitet das Team konzentriert und ohne Störungen von außen daran, die Tasks aus dem Sprint Backlog in ein Increment of Potentially Shippable Functionality, also einen vollständig fertigen und potentiell produktiv einsetzbaren Anwendungsteil, umzusetzen. Das Team gleicht sich in einem möglichst täglichen, streng auf 15 Minuten begrenzten Informations-Meeting, dem Daily Scrum Meeting, ab, damit jeder weiß, woran der andere zuletzt gearbeitet hat, was er als nächstes vor hat und welche Probleme es evtl. Gibt

Am Ende des Sprints präsentiert das Team dem Product Owner, den Stakeholders u.a. interessierten Teilnehmern in einem sog. Sprint Review Meeting live am System die implementierte Funktionalität. Halbfertiges oder gar Powerpoint-Folien sind während des Reviews verboten. Das Feedback aller Beteiligten und Stakeholders und die neuen Anforderungen des Product Owners für den kommenden Sprint fließen dann wieder in das nächste Sprint Planning Meeting ein, und der Prozeß beginnt von neuem.