ITSM MAGAZIN

ISSN 1861-9258 14€
9771861925009
Ausgabe 02/2024

Security by Service-Design
Problemlösung als Schlüsselkompetenz
Wegweiser zur Automatisierung im IT- Service Management

MODERNE IT ABTEILUNGEN

SECURITY BY SERVICE DESIGN

Bilden Service Management und Information Security Management das Dream-Team zur dauerhaften Gewährleistung des Sicherheitsniveaus? Der Security by Service-Design (SxSD) Ansatz adressiert, dass Security in allen Bereichen des Service Managements mitgedacht und mitgelenkt wird – und sorgt so dafür, dass Sicherheit von der ersten Idee eines neuen Service über die Inbetriebnahme und den Regelbetrieb bis zur Außerbetriebnahme gewährleistet wird.

Von Martin Glaser, Andreas Dassen, Franz Gläser und Robert Manuel Beck

Trotz allgegenwärtig zunehmender Sicherheitsvorfälle wird Security meist immer noch in einem von zwei Modi betrieben: entweder nach dem Gießkannenprinzip der Compliance (Gleiches Maß an Sicherheit für alle Services & Anwendungen) oder nach der Rettungsdienstlogik (Vorfall -> Management Attention -> Aktivismus), bisweilen mühsam getarnt durch das Label der Risikobasiertheit. Bei vielen Unternehmen folgt das IT-Sicherheitsprogramm noch keinem systematischen Grundsatz .

In der Softwareentwicklung ist **Security by Design** ein wichtiges Paradigma, das hilft, Sicherheit frühzeitig und ganzheitlich im Code zu verankern. Dies zielt jedoch in der Regel auf **einzelne Produkte** ab, ist damit aufwendig, immer individuell umzusetzen und vor allem auf die Entwicklungsphase am Anfang des Lebenszyklus beschränkt. Der Ansatz **Security by Service Design** erweitert das Konzept von der Softwareentwicklung auf den gesamten Lebenszyklus der Services, mithin Einsatzzweck und Daseinsberechtigung der Produkte, also die Service-Erbringung. Für die betriebenen und angebotenen **Services** kommt somit eine angemessene **Security**, nicht mehr zufällig heraus, sondern wird kontinuierlich an neue Bedrohungen, Technologien oder sonstigen veränderten Anforderungen angepasst.

VERANKERUNG IN DER SERVICE-ERBRINGUNG

Es existiert in der Praxis oftmals kein abgestimmtes Vorgehen zwischen **Service Management** und **Information Security Management**:

Solange diese Trennung von **Service Management** und **Security** fortbesteht, finden im Prinzip zwei getrennte Kämpfe gegen dieselben Windmühlen statt. In Kombination mit fehlendem Business-Know-how auf beiden Seiten führt das dazu, dass die Ziele einerseits nicht aufeinander abgestimmt sind, andererseits Business-Anforderungen immer wieder individuell abgeholt werden müssen. Das wirkt auf alle Beteiligten im Geschäftsprozess dauerhaft zermürbend.

Es fehlt also an einer Vorgehensweise, um die **Serviceerbringung** systematisch, ganzheitlich und dauerhaft mit der **Security** in das gesamte Service-Portfolio einfließen zu lassen.

Andersherum wäre es hilfreich, **Security** als Kosten- und Nutzenfaktor durch das **Service Management** sicht- und messbar zu machen. Das wiederrum, um die Kosten zu optimieren und den konkreten Nutzen für das Business herauszustellen.

Dafür ist ein **„Shift Left“** im Sinne einer Vorverlagerung analog zum Bereich der Softwareentwicklung notwendig. Dort hat das Konzept bereits

einen großen Rückhalt. **Security** muss also von Anfang an in die Diskussion mit dem Kunden einfließen. Das verlangt nach einem intensiven Abgleich mit dem Business. So wird das richtige **Maß an Sicherheit** für jeden Service über den gesamten Lebenszyklus aufgebaut und aufrechterhalten. Dadurch werden Risikobasiertheit, Wirtschaftlichkeit und Nachhaltigkeit zu Qualitätskategorien. Über diese wird mit Kunden verhandelt und nicht zuletzt auch die Preisfindung betrieben. Gelingen kann das jedoch nur durch tiefe Integration in andere Qualitätsprozesse und die eingesetzten **Service Management Frameworks**.

Ist die Zusammenarbeit erfolgreich, ergibt sich für **Information Security Management** eine höhere **Sicherheit**. Denn das gewünschte Risikoniveau im Betrieb ist dauerhaft gewährleistet. Das garantiert reduzierten Stress durch weniger **Feuerwehreinsätze** und eindeutige Verantwortlichkeiten. Aufseiten des **Service Managements** lässt sich eine erhöhte **Kundenzufriedenheit** erzielen sowie gegebenenfalls auch ein Alleinstellungsmerkmal auf dem Markt produzieren.

DAS NEUE DREAM-TEAM

Wenn es also gelingt, die Ziele von **Service Management** und **Information Security Management** aufeinander abzustimmen, kann eine Kette von Sicherheitsanforderungen vom **Kunden des IT-Services** bis hin zu den von den einzelnen **IT-Bereichen** erbrachten Services abgebildet werden.

Dafür müssen Kunden beantworten welche Anforderungen an Vertraulichkeit, Integrität, Verfügbarkeit und weitere Werte der im **Service** verarbeiteten Informationen zu stellen sind. Durch Konkretisierung und Einstufung des Schutzbedarfs in einem **Service-Level-Agreement** (SLA) lassen sich dann reale Maßnahmen in der Serviceerbringung definieren. Das **Service-Modell** muss dafür das Wissen bereitstellen, welche Bereiche innerhalb der IT an der Leistungserbringung eines jeden Services beteiligt ist. Die **Servicekomponente** wird durch die Unterstützung von **Information Security Management** in Maßnahmen pro Bereich definiert. Damit wird das jeweilige Sicherheitslevel gewährleistet. Dazu stellt der **Service-Manager** mit Unterstützung durch **Information Security Management** sicher, dass das benötigte Sicherheitsniveau auch im Zusammenspiel der unterschiedlichen **Servicekomponenten** eingehalten wird.

Die Sichtweise des **Security by Service Designs** ist folgende: Angestrebt wird die verlässliche Sicherheit des **Services**, während seines gesamten Lebenszyklus – alle Beteiligten und Stakeholder dabei zu berücksichtigen ist eine Selbstverständlichkeit, egal ob sie innerhalb oder außerhalb der Organisation angesiedelt sind.

Um das zu erreichen, muss das **Service Design** explizit auch Sicherheitsfragen berücksichtigen, dabei sowohl Bedrohungen von außerhalb der Organisation als auch die oftmals ignorierten internen Risiken beachten und sich vor allem in einer frühen Phase der Einführung und Entwicklung einbringen. Zusammenfassend gesprochen: Das **Service Management** muss alle vier Quadranten der von den Phasen Einführung und Betrieb sowie von externen und internen Bedrohungsquellen aufgespannten **Matrix** betrachten.

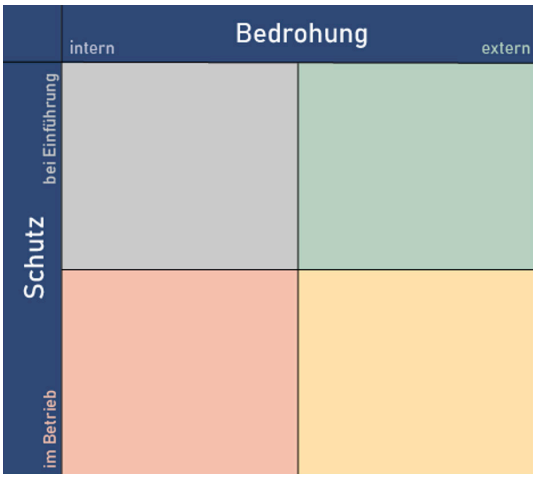

Abbildung 1:
Bei Sicherheitsbetrachtungen zu Services gilt es, die Phasen von Einführung und Betrieb sowie Bedrohungen von intern wie extern zu beachten.

Fazit - Mittels **Security by Service Design** wird über den gesamten Service Lifecycle ein angemessenes Level an Sicherheit gewährleistet. So werden Potenziale für Sicherheitsverbesserungen aktiv gestaltet. Das Mittel dazu ist das **Service Design**, oder umfassender gedacht: das **Service Management.**

Dank **Security by Service Design** können mithilfe des im **Service Management** kanalisierten Business-Know-Hows (wo?) gemeinsam mit der technischen Expertise der Security (wie?) Bedrohungen deutlich besser abgewehrt werden. Damit wird durch die Zusammenarbeit von **IT-Service Management** und **Information Security Management** Sicherheit effizienter auf das angestrebte Niveau gebracht.

Martin Glaser
Diplom Informatiker

ist seit über 15 Jahren im Umfeld IT-Service Management unterwegs mit den Schwerpunkten: Service Engineering, Service Strategy und Service Design. Die von ihm verantworteten Projekte begleiten die IT-Service Manager:innen dabei im gesamten Service-Lebenszyklus, vom Design des Service-Modells und des konkreten Service über die Transition neuer Services bis zur Optimierung des Service Managements der betriebenen Services. Die beinhaltet insbesondere auch Security Aspekte und Sourcing Fragestellungen.

HISOLUTIONS

Sicher. Besser. HiSolutions ist eine führende Management- und Technologie-Beratungsgesellschaft für Sicherheit und Digitalisierung. Seit über 30 Jahren kombinieren wir hochspezialisiertes Know-how mit Konzeptionsstärke, Innovationskraft und Umsetzungskompetenz. Über 300 Mitarbeitende an fünf Standorten unterstützen Unternehmen und Institutionen nahezu aller Branchen sowie die öffentliche Verwaltung in Bund, Ländern und Kommunen dabei, die Chancen des digitalen Wandels für sich zu nutzen und die damit verbundenen Risiken zu beherrschen. In mehr als 1.100 Projekten jährlich werden Grenzen und Barrieren in der Zusammenarbeit von Business und IT abgebaut und wirkliche Business-IT-Partnerschaften entwickelt.

HISOLUTIONS

Informationssicherheit & Service Management als neues Dream-Team:

Security by Service Design.

Sind Ihre Services „konstant sicher“? Mit Security by Service Design wird das Zusammenspiel von Informationssicherheit und Service Management auf eine neue Ebene gehoben. Angestrebte Sicherheitsniveaus für IT-Services werden über deren gesamten Lebenszyklus, von der Implementierung bis zur Außerbetriebnahme, mitgedacht und gesteuert. Im Ergebnis werden die Ziele aller Beteiligten – vom CISO bis zum Service Manager – schneller und besser erreicht.
Das gilt auch für die Umsetzung der NIS2 Anforderungen.

HiSolutions. Sicher. Besser.

NIS2 kommt.

Der Kompass von HiSolutions zeigt Unternehmen, ob und wie sie handeln müssen.
Ca. 29.000 deutsche Organisationen werden von NIS2 betroffen sein. Wir beraten und begleiten Sie bei der praktischen Umsetzung.

Zum NIS2-Kompass:

HiSolutions AG | Berlin | Frankfurt | Bonn | Düsseldorf | Nürnberg

www.hisolutions.com

itSMF
Wir sind die Service Manager:Innen

ITSM
IT Service Management Kongress
2024

Gemeinsam. Stark. Zukunftssicher.

18./19. November 2024 | GOP Variete | Bonn

itSMF

Wir sind die Service Manager:Innen

Wir freuen uns auf Sie!

Besuchen Sie unsere Homepage, stöbern Sie in unserem Blog und nehmen Sie Kontakt mit uns auf. Wir freuen uns darauf, Sie als wertvolles Mitglied unserer Community begrüßen zu dürfen.

itSMF.de

www.itsmf.de