probicon
> business services <

pro : b
Process und Change Management

Infoletter 2/14

Informationssicherheit im Unternehmen als ganzheitlichen Prozess implementieren

Jürgen Marx

Informationen in Unternehmen sind schützenswerte Güter. Ihre Sicherheit vor beabsichtigten oder zufälligen Zugriffen durch Unbefugte zu gewährleisten, ist nach wie vor in vielen mittelständischen Unternehmen ein ungelöstes Problem. Das gilt auch für Großunternehmen und Institutionen. Nicht einmal Geheimdienste schaffen es, ihre Geheimnisse vor dem Zugriff Unbefugter zu sichern. Der Wettlauf von/zwischen Hackern und Informationsschützern erinnert an den zwischen Hase und Igel.

Wer sich krimineller List erwehren will, sollte Informationssicherheit im Unternehmen nicht mit Patentrezepten schützen. Einzelne Initiativen können Ihre Wirkung nur dann voll entfalten, wenn sie Hand in Hand gehen, wenn sie Ergebnis einer ganzheitlichen Betrachtung sind. Informationssicherheit als ganzheitlicher Prozess setzt an der Klassifikation der Unternehmensdaten an und es muss eine ganze Reihe von Fragen nacheinander beantwortet werden. Hier einige Beispiele:

- Welche Informationen sind schützenswert, weil sie intern, vertraulich, geheim oder überlebenswichtig sind?
- Wie kann man diese Informationen adäquat und bezahlbar schützen?
- Ist den Kollegen oder Mitarbeitern, die mit den Informationen im Büroalltag umgehen, die Bedeutung der Informationen bewusst?
- Wie werden bereits existierenden Regeln und Vorschriften eigentlich von den Mitarbeitern „gelebt"?
- Ist den Mitarbeitern ihre Verantwortung im Umgang mit sensiblen Informationen bewusst?

Am einfachsten klärt man diese Fragen in einem kurzen Assessment Vorort. Mit dem so gewonnenen Wissen bzw. einer aussagekräftigen Status-Quo-Beschreibung lassen sich danach auch die nachgelagerten Prozessschritte optimieren, wie z.B. die Speicherung, Übermittlung und Nutzung der Informationen bei Firmenangehörigen, Partnern und Kunden betrachtet werden.

Sowohl für die Durchführung geeigneter Assessments, wie auch für die anschließende Prozessoptimierung können wir mit unserer langjährigen Erfahrung mit Rat und Tat zur Seite stehen.

Wie sehen Lösungsansätze aus unserer Praxis aus?

Informationssicherheit im Unternehmen muss von allen Mitarbeitern „gelebt" werden. Zuerst gilt es, für das Thema kompetente Ansprechpartner, in größeren Organisationen sogar eine dedizierte „CISO" (Chief Information Security Officer) Rolle in der Organisation zu installieren. Der CISO überwacht Umsetzung und Einhaltung der unternehmensweiten Informationssicherheitsinitiativen. Um notwendige Veränderungen auch herbeiführen zu können, muss diese Rolle „ermächtigt", also in die entsprechenden Unternehmensprozesse eingebunden werden.

In den für Informationssicherheit zu entwickelnden Konzepten muss jedes Sicherheitsrisiko im Unternehmen Berücksichtigung finden. Es gilt, alle Vorgänge der Datenerhebung, -verarbeitung und –nutzung kritisch zu überprüfen. Alle Vorgänge der Datenerhebung, Verarbeitung und Nutzung gilt es, kritisch zu überprüfen. Im Abgleich mit der IT-Infrastruktur im Unternehmen werden sodann Server, Betriebssysteme und die jeweilige Software unter die Lupe genommen, um zu einem ver-

Editorial

Informationen stellen heute für Unternehmen einen hohen Wert dar. Sie zu schützen ist – auch angesichts der aktuellen Gesetzeslage – eine unumgängliche Notwendigkeit.
Wie lassen sich Sicherheit und Zuverlässigkeit der im Unternehmen eingesetzten Informationstechnik gewährleisten? Und vor allem: Wie können Mitarbeiter für einen verantwortungsvollen Umgang mit Informationen und zur Beachtung entsprechender Sicherheitsvorschriften gewonnen werden?
Unser Infoletter zu dieser Thematik will den Weg aufzeigen, auf dem im Rahmen eines methodisch zu entwickelnden Informationssicherheitskonzeptes im Unternehmen ein zielgerichteter Prozess zur Sicherung von Daten und Informationen auf- und umgesetzt werden kann.
Das Gespräch mit Herrn Reihl zeigt beispielhaft, wie in der Praxis ein angemessenes Sicherheitsniveau erreicht und nachhaltig aufrechterhalten werden kann.

Jürgen Marx

lässlichen Urteil über den Status der Informationssicherheit im Unternehmen zu gelangen.

Um ein unternehmensgemäßes, „wasserdichtes" Informationssicherheits-Konzept zu entwickeln, es ist unerlässlich, Übersicht zu gewinnen und Ordnung in den Prozessen der Informationssicherheit zu schaffen. Dessen erfolgreiche Umsetzung setzt voraus, dass Fragen von Governance & Compliance geklärt, also Vereinbarungen in Leit- und Richtlinien sowie Regelungen getroffen werden. Auch die Kommunikation muss geregelt sein, Kenntnisse müssen vermittelt und Kontrollinstanzen etabliert werden. Es gilt letztlich, dass durch Schulungs- und Trainingsmaßnahmen das notwendige Informationsschutz-Bewusstsein und die entsprechenden Verhaltensänderungen erreicht werden.

Bei der Statuserhebung, wie auch bei der Entwicklung und nachhaltigen prozessualen Umsetzung von Informationssicherheits-Konzepten, stehen wir als erfahrene Berater und Moderatoren zur Verfügung. Mit dem Ziel, für die Sicherheitsprobleme im Unternehmen zu sensibilisieren, bei ihrer Lösung beratend mitzuwirken und vorhandene Ansätze zu optimieren. Vom Assessment über die Erstellung von Maßnahmenkatalogen bis hin zur Definition von Prozessen und Standards zum Ausgleich von Sicherheitsdefiziten können wir kleineren und mittleren Unternehmen in dem dafür erforderlichen Veränderungsprozess hilfreich zur Seite stehen.

Aus der Praxis der Informationssicherung

Wir fragen
Hans Reihl, Projektleiter für die Konzeption und Durchführung von Informationssicherheits-Assessments im Volkswagenkonzern

Herr Reihl, Sie gehören zu den gefragten Experten, die sich nicht nur erst seit Bekanntwerden brisanter Spionage-Affären mit der Praxis der Informationssicherung in Unternehmen befassen. Reicht hier der Einsatz der inzwischen hoch entwickelten Technik des Datenschutzes nicht aus?

Es hat sich gezeigt, dass Informationen im Unternehmen nur so sicher sind, wie es das Verhalten der mit ihnen im Unternehmen arbeitenden Menschen erlaubt. Technische Sicherheit schützt vor Angriffen von außen, hilft aber nicht bei Bedrohungen, die von der eigenen Organisation – also von innen – ausgehen. Egal ob gewollt oder ungewollt.

So, wie Airbags, Abstandswarner und Totwinkelassistenten allein aus einem riskanten Autofahrer keinen risikobewussten Verkehrsteilnehmer machen werden, bedarf es einer Einstellungsveränderung, eines veränderten „mindsets". Und der Weg dorthin ist ein Prozess, der in jedem Fall die aktive Mitarbeit des Betreffenden erfordert.

Welche Eckpunkte muss Ihr Team berücksichtigen, um im Unternehmen das notwendige Sicherheitsbewusstsein und die neuen Verhaltensweisen durchzusetzen?

Immer ausgehend von der Tatsache, dass alle Initiativen zur Sicherung von Informationen nur dann zielführend sein können, wenn die Mitarbeiter mit Daten und Informationen verantwortungsbewusst umgehen:

Zuerst werden die Ziele des Unternehmensschutzes festgelegt. Daraufhin werden zweitens die entsprechenden Konzepte entwickelt, überarbeitet und aufgesetzt. Drittens gilt es nun die Mitarbeiter für die Gefahren zu sensibilisieren, über die geplanten Maßnahmen zu informieren und den sicheren Umgang mit Informationen zu schulen. Schließlich müssen viertens die Umsetzungsqualität über Key Performance Indicators (KPIs) kontrolliert, die angestrebten Resultate nachgehalten und notfalls eingefordert werden.

Und was lässt sich über die Resultate sagen?

Wir haben diesen Prozess für unseren Auftraggeber im Verlauf von vier Jahren durchgeführt, weltweit an mehr als 100 Standorten. Damit haben wir – die KPI's sprechen dafür – die Unternehmenswelt in Sachen Information erheblich sicherer gemacht.

Welche Erkenntnisse konnten Sie bei der Praxisarbeit hinzugewinnen?

Vor allem: Informationssicherheit muss bei verteilten Organisationen dezentral organisiert werden. Die einzelnen Standorte brauchen ein hohes Maß an Autonomie, um die Informationssicherheitsziele adäquat und ihren Bedürfnissen gerecht umsetzen zu können. Dabei sollte sich Kommunikation, die vom Hauptquartier ausgeht,

auf die Vorgabe der Schutzziele und die qualitative und terminliche Kontrolle der Umsetzung konzentrieren.
Die Kommunikation von Ergebnisberichten oder KPIs, Veränderungen, Unterstützungsbedarf (Schulungen, Consulting), Verbesserungsprozessen und der Erfahrungsaustausch wie auch die Umsetzungskontrolle (qualitativ und quantitativ) sollte dezentral durch die Prozesse und Verantwortlichen am Standort erfolgen.

Unser nächstes pro : b - Schwerpunktthema

In unserem nächsten Infoletter befassen wir uns mit der Bedeutung von Change Management bei IT-Projekten und dessen Einfluss auf den Unternehmens- bzw. Projekterfolg.

Die Themen der bisher erschienenen pro : b - Ausgaben:

01-14: Business Transformation: Wachstumspotenzial nutzen - Vertriebsorganisation stärken!
02-13: Unternehmensstrategien erfolgreich umsetzen
01-13: Begleitendes Change Management bei der Einführung von agilen Entwicklungsmethoden
04-12: Outsourcing heute: Mehr Flexibilität, mehr Transparenz, mehr Möglichkeiten
03-12: Neue Unternehmensstrategien (be)greifbar machen
02-12: Widerstände und Konflikte in Veränderungsprojekten
01-12: Globale Standardisierung von Prozessen
04-11: Change und Rollout-Management
03-11: Komplexitätsmanagement in wachsenden Unternehmen
02-11: Veränderungsmanagement in mittelständischen Unternehmen
01-11: Optimierung von End-to-End-Prozessen von Unternehmen
04-10: Selbstorganisation in IT-Projekten
03-10: Das richtige Team für das Veränderungsprojekt
02-10: Prozessoptimierung in IT-Projekten
01-10: Transformation der Unternehmensstrategie in Prozesse und Organisation

Die bisher erschienenen Ausgaben finden Sie auch unter http://business-engineering.probicon.de/infoletter.html
Für Informationen und Anfragen: Jürgen Marx

Unsere Autoren

Dipl.-Wi.-Ing. Jürgen Marx ist geschäftsführender Gesellschafter der probicon GmbH in Berlin. Er besitzt umfangreiche und langjährige Erfahrungen in der Organisations- und Managementberatung. Jürgen Marx berät namhafte Firmen unterschiedlicher Branchen in den Gebieten Business Transformation, Business Process Management, Change Management und IT Consulting.

Dipl.-Wi.-Ing Hans Reihl hat rund 20 Jahre Berufserfahrung als Consultant und Projektleiter. Schwerpunkte seiner Beratungstätigkeit sind Organisations- und Prozessoptimierung, Restrukturierung und Change Management, Strategieentwicklung und Marktanalysen sowie analytische Methoden für die verschiedensten Produktions- und Dienstleistungsindustrien.

Impressum

probicon GmbH
Mehringdamm 40
10961 Berlin
Tel.: 030 / 805 86 99-0
consulting@probicon.de
http://business-engineering.probicon.de