Auf Nummer sicher – physische Sicherung von radioaktiven Materialien

Jörg SCHULZ [1]
[1] Von zur Mühlen'sche GmbH, Bonn

Kontakt E-Mail: js@vzm.de

Kurzfassung: Die Absicherung radioaktiven Materials ist von elementarer Wichtigkeit: in die falschen Hände gelangt kann einiges angerichtet werden. Vieles ist möglich, aber nicht alles nötig. Bevor überstürzt in Maßnahmen der physischen und technischen Sicherung (wie z. B. Zäune, Einbruchmeldeanlagen, Videoüberwachung, etc.) investiert wird, sollten systematisch die Umgebungsbedingungen analysiert und im Rahmen einer Risikoabschätzung Vorannahmen zu potentiellen Gefährdungen getroffen werden. Als erste Annäherung verdeutlicht das so genannte Zwiebelschalenmodell, wie der Notwendigkeit nach physischer und technischer Sicherung strukturiert entsprochen werden kann. Ähnlich den Schalen einer Zwiebel lassen sich bestimmte Schutzzonen nach dem Ausmaß des Schutzbedarfs (z. B. Einbruchswahrscheinlichkeiten) definieren. Danach können pragmatische und effiziente Lösungen zur Absicherung gesucht werden, die sich an dem konkreten Schutzbedarf ausrichten und mit den darauf aufbauenden organisatorischen Prozessen in Einklang gebracht werden können. So vermeidet man ein „mit Kanonen auf Spatzen schießen“ und erhält ein ganzheitliches Sicherheitskonzept mit aufeinander abstimmten Maßnahmen. Mit dieser Methodik erreichen Sie das wirklich benötigte Maß an physischer und technischer Sicherheit, was im Idealfall auch finanzielle Einsparungen bedeuten kann.

Einführung

Das Thema Sicherheitsmanagement kommt in Unternehmen und Organisationen mehr und mehr da an wo es hingehört; Nämlich auf der Ebene der Entscheidungsträger, Unternehmenslenker und Führungskräfte. Dies ist das Resultat eines jahrelangen Prozesses der Bewusstseinsbildung, die das Thema Sicherheit herausholt aus Ebenen der Belanglosigkeiten und der Nebensächlichkeiten, ein Wandel hin zu einem wichtigen Business Enabler für reibungslose Geschäftsprozesse.

1. Ganzheitlichkeit

Der gesamte hier behandelte Themenkomplex muss von Beginn an durch Ganzheitlichkeit geprägt sein. Jede Technik und jedes System hat seine Stärken aber auch seine technologisch bedingten Grenzen. Diese sind mit anderen Lösungen aufzufangen und hier darf keineswegs nur über Technik nachgedacht werden. Denn die Basis für alles weitere sind nach wie vor bauliche und konstruktive Maßnahmen. Und damit aus Konstruktion und Technik ein erfolgreicher Prozess wird, sind personelle und organisatorische Maßnahmen obligatorischer Bestandteil einer erfolgreichen Gesamtlösung. Ganzheitlichkeit heißt das Stichwort. Jedoch

kann nie irgendeine Sicherheitstechnik eine fehlerhafte bauliche Situation auffangen genau wie organisatorische Maßnahmen nicht dazu dienen dürfen, mangelhafte bauliche und technische Umstände zu kompensieren.

Wer Maßnahmen plant, braucht Schutzziele, die ihm die Angemessenheit der Maßnahmen aufzeigen und ein ständiges Überprüfen/Plausibilisieren der Maßnahmen ermöglichen. Wer Schutzziele formulieren will, muss dies im Bewusstsein der individuellen Risikolage tun, um die Schutzziele nicht an der Bedrohungslage vorbei zu definieren. Dies ist bekannt und bewährt. Und diese bewährte Strategie gilt es definitiv weiter anzuwenden und mit modernen Werkzeugen fortzuschreiben.

2. Deming-Kreis

Eine Methodik dazu wäre der Deming-Kreis mit seinem Zyklus PLAN-DO-CHECK-ACT. Diese in vielen Bereichen bereits anerkannte und bewährte Methodik kann man ohne weiteres im Kontext Sicherheitsmanagement anwenden. Hierbei muss man keineswegs das Rad neu erfinden, denn die beschriebenen systematischen Schritte lassen sich innerhalb des Deming-Kreises zuordnen und um den wichtigen Schritt der ständigen Evaluierung erweitern. So kann Bewährtes weiter angewendet und um zeitgemäße Aspekte erweitert werden, indem man innerhalb der einzelnen Schritte die folgenden Handlungen durchführt:

2.1 Plan

Risiken und Bedrohungen sind zu analysieren, indem man Eintrittswahrscheinlichkeit und potentielle Schadenshöhe auf einer Skala beispielsweise von 0 - 5 einsortiert und aus dem Produkt der beiden Aspekte eine objektivierte Risikoeinschätzung vornimmt. Anhand dieser Betrachtung kann relativ unmissverständlich erkannt werden, welchem der beiden Aspekte mit Maßnahmen am wirkungsvollsten entgegengewirkt werden kann.

Ziele sind zu benennen, indem man aus den Ergebnissen der Risikoanalyse heraus die Schutzziele definiert und sie gewissermaßen als Vision für alle weiteren Planungen ganz oben anstellt. Verbleibende Restrisiken müssen benannt und ins Bewusstsein gerückt werden, damit Entscheidungsträger in der Lage sind abzuwägen. Wer Investitionen scheut, kann oft ein bestimmtes Schutzziel nicht erreichen und wirkt somit einem bestimmten Risiko nicht entgegen. Diese Bewusstseinsbildung hilft bei Investitionsentscheidungen, Budgets zu plausibilisieren und zu begründen.

Sicherheitsvorgaben und Standards sind zu formulieren, indem man aus den Schutzzielen bestimmte immer wiederkehrende allgemeingültige Definitionen ableitet und granularer benennt. Konkrete Maßnahmen sind zu planen, indem in dieser Ebene Lösungen mit Einzeltechniken und Sensoriken entwickelt werden die den Risiken entgegenwirken, sei es durch baulich/mechanische Härtung, meldetechnische Signalisierung und Überwachung oder personelle organisatorische Prozesse.

2.2 Do

Maßnahmen sind umzusetzen, indem durch Fachplaner bauliche und technische Lösungen ausführungsreif geplant und ausgeschrieben und diese dann durch Fachunternehmer umgesetzt werden. An dieser Stelle bietet sich die Option einer Proof-of-Concept-Phase an, die nicht immer zwingend notwendig ist, jedoch gerade bei komplexen Anwendungen vor dem großen Rollout Stärken und Schwächen aufzeigen kann. Systeme sind zu aktivieren,

indem die installierten Lösungen in Betrieb genommen, getestet und an den Betreiber übergeben werden.

2.3 Check

Die Wirksamkeit der Maßnahmen ist zu prüfen, in dem ein Abgleich der zuvor definierten und vereinbarten Schutzziele vorgenommen wird und eine Erreichung der Schutzziele überprüft wird. Abweichungen sind hierbei festzustellen und zu beheben, in dem ein laufendes Verfahren der Erfassung und Kontrolle etabliert wird.

2.4 Act

Die Zielerreichung ist permanent zu prüfen, indem die vorgenannten Aktivitäten nicht nur nach der Inbetriebnahme vorgenommen werden, sondern als kontinuierlicher Prozess und als wiederkehrende Handlung.

Auch die Ziele sind permanent zu prüfen, indem ebenfalls als wiederkehrende Handlung festgestellt wird, ob die Schutzziele noch richtig definiert sind oder ob durch veränderte innere oder äußere Einflüsse eine Anpassung notwendig ist. Sollten hierbei größere Abweichungen festgestellt werden gilt es, den PDCA-Zyklus neu zu starten und den Gesamtprozess erneut zu durchlaufen.

Bemerkenswert an dieser Betrachtung ist, dass sich an die initiale Phase, die durch Risikoanalyse, Schutzzieldefinition und schlussendlich dem Umsetzen von Maßnahmen geprägt ist, eine Phase des Betriebes und der Instandhaltung anschließt.

Weiter aufgedröselt meint Evaluierung hierbei zuerst, dass sich an die genannten Phasen ein Schritt der interoperablen Funktionstests anschließt. Innerhalb solcher Tests ist nachzuweisen, dass die Integration unterschiedlicher Lösungen, Systemtechniken und Gewerke erfolgreich umgesetzt wurde und sich so aus einer Vielzahl von Einzeltechniken eine homogene Gesamtlösung ergibt. Geprägt sind solche Tests durch eine Sichtweise, die nicht in Systemtechniken oder Anlagen denkt, sondern in Prozessen und Szenarien. Dies können Angriffs-, Sabotage- oder Bedrohungsszenarien sein, deren Abwendung bereits in den Schutzzielen definiert sein müsste. Nun gilt es, diese Szenarien so realitätsnah wie möglich darzustellen und auch auszuführen, um die Wirksamkeit der Maßnahmen als Ganzes zu prüfen und zu beurteilen. prüfen.

Dem Verfahren vorauszugehen hat natürlich ein 1:1-Test der einzelnen Anlagen als Nachweis der vollen Funktionsfähigkeit und Einsatzbereitschaft. Bestenfalls gelingt es so, mit den Integrationstests eine ganzheitliche Wirkungsweise sowohl der baulichen Anlagen, der technischen Systeme sowie der folgenden organisatorischen Maßnahmen nachzuweisen. Es versteht sich aber von selbst, das hier von Ausnahmen abgesehen nur zerstörungsfrei prüfbare Systeme und Anlagen berücksichtigt werden können. Kaum einer würde innerhalb eines solchen Tests auf die Idee kommen, eine Scheibe einzuschlagen oder eine Tresorwand zu durchbrechen. Auch Blitzschutzsysteme lassen sich kaum mit solchen Methoden prüfen.
Sind interoperable Funktions- und Integrationstests erfolgreich abgeschlossen, begibt man sich in die wohl längste Phase einer Sicherheitslösung nämlich die Betriebsphase. Gewöhnlich werden sicherheitstechnische Anlagen und Systeme durch Instandhaltungsleistungen gepflegt und über Jahre funktionsfähig gehalten. Diese Instandhaltungsleistungen können vorbeugenden oder korrektiven Charakter haben und gliedern sich üblicherweise in Inspektion, Wartung, Instandsetzung und Verbesserung.

Erweiternd kann auch hier der Gedanke eines kontinuierlichen Zyklus´ dazu genutzt werden, einen Schritt weiterzugehen: Nicht nur die Technik an sich muss am Leben erhalten werden, sondern auch die Erreichung der ursprünglich gesteckten Schutzziele ist permanent zu hinterfragen. Ebenso gehört eine ständige Fortschreibung sowie Anpassung der Ziele durch veränderte Risiko- und Gefährdungslagen dazu.

3. Fazit

Wenn man also wie beschrieben eine erfolgreiche Initialphase in einen laufenden Prozess überführt hat man beste Chancen, dass die Lösung für lange Zeit die gesteckten Ziele erreicht und zum Unternehmenserfolg beiträgt.