

Zählen – Messen – Wiegen

oder: Wie kann ich meine IT-Security messbar machen?

Die Frage nach der Messbarkeit von Informationssicherheit ist fast so alt wie der Gedanke an Informationssicherheit selbst. Mit dem „Open Source Security Testing Methodology Manual“ (OSSTMM) von der Herausgeberin „Institute for Security and Open Methodologies“ (ISECOM) wurde bereits vor einiger Zeit ein erster Ansatz erstellt, der nunmehr durch intensive Forschungsarbeit weiterentwickelt wurde und in dieser Frage einen großen Schritt in die richtige Richtung darstellt. So wird mit Hilfe des in OSSTMM integrierten Risk Assessment Values (RAV) IT-Sicherheit eine exakte Wissenschaft. Das weltweit einzige Sicherheitstesthandbuch liefert mit dem RAV einen integralen Bestandteil, der Kennzahlen als Grad der Zielerreichung für Informationssicherheit liefert. Der faktenbasierte RAV kann so die Wirksamkeit von Sicherheitsmaßnahmen tiefgehend messen und gleichzeitig ergänzend zur klassischen Risikoanalyse genutzt werden.

Der RAV bildet so die Grundlage für ein quantifizierbares IT-Sicherheits-Management mit einem Nutzen stiftenden Controlling-Framework zur Bemessung von Wirksamkeit, Nachhaltigkeit sowie dem Finanzbedarf von Informationssicherheit.

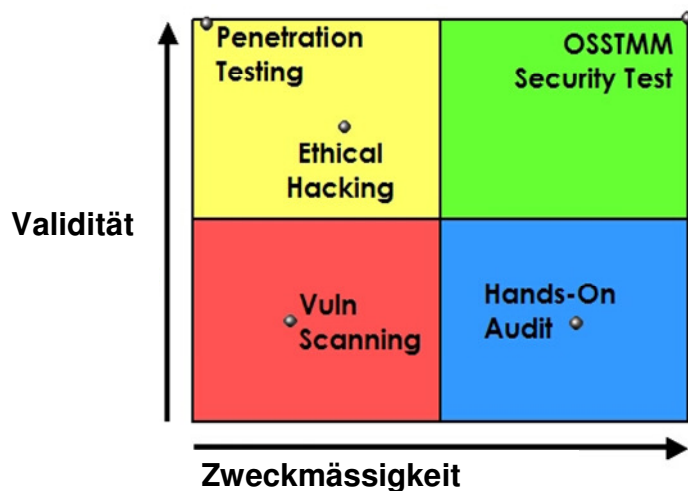


Abbildung 1 Positionierung

Zusammenspiel der Sicherheitswelten

Insgesamt stellt sich bei der Messung von IT-Sicherheit die Frage, inwieweit technische und organisatorische Sicherheit gemessen werden können. In zunehmend verstärktem Maße nimmt die Fragestellung, wie die IT-Compliance faktisch gemessen werden kann an Bedeutung zu. In verstärktem Umfang erleben die Informations-Sicherheitsspezialisten der adMERITia, dass Geschäftspolitik und Sicherheitspolitik nicht mehr konträr zueinander stehen sondern sinnvoll und intelligent miteinander verknüpft werden können, ja sogar müssen.

Die Methodologie von OSSTMM sorgt mit ihrer subjektiven und finanziellen Messung von operativer Sicherheit für eine gründliche Analyse der operativen und strategischen Ebene, so dass durchgängig vom Geschäftsprozess bis zur Konfiguration von IT-Systemen die notwendige Sicherheit bestimmt und das Sicherheitsniveau präzise und zunächst bestimmt und dann zuverlässig gemessen werden kann.

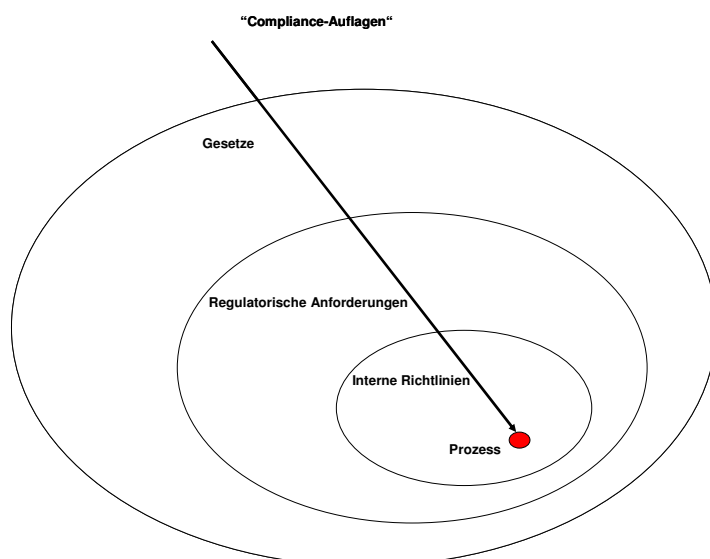


Abbildung 2 OSSTMM-Compliance

Auf diese Weise erhält IT-Sicherheit ebenso wenig Selbstzweck-Charakter, wie Informationstechnologie selbst. Viel mehr wird mit Hilfe der Sicherheitsmetrik RAV des OSSTMM festgestellt, welcher Prozess welche Sicherheit benötigt. Dabei rückt das heutzutage leider immer noch vorrangige Denken in „Security Tools“ deutlich in den Hintergrund, so dass sich ein pragmatisches Profil der Informationssicherheit abzeichnet.

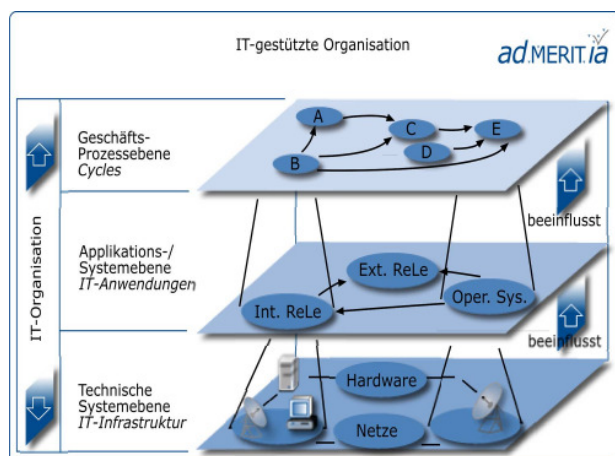


Abbildung 3 Prozesssicherheit

Verantwortung für Sicherheit

Die Sicherheitstester und Auditoren der adMERITia erleben im praktischen Unternehmensumfeld häufig unterschiedliche Regelungen von Informationssicherheit, wobei der Grundsatz aufgestellt werden kann, dass je kleiner das Unternehmen, aber auch je weniger die Geschäftsprozesse von Informationstechnologien und ihrer Sicherheit abhängig sind, die Verantwortungsregelung um so diffuser wird.

Dabei ist unter Berücksichtigung des Grundsatzes „Separation of Duties“ grundsätzlich egal, wer die Verantwortung für Informationssicherheit trägt, Hauptsache die Verantwortung ist klar geregelt und mit einem Mandat zur Durchsetzung von Informationssicherheit verbunden. In der Regel findet sich in der Unternehmenslandschaft ein stark begrenztes

Budget für den Sicherheitsverantwortlichen. Hier helfen die integralen Ansätze von OSSTMM um z.B. Antworten auf die Frage, wie viel Geld sollte das Unternehmen in IT-Sicherheit investieren, geben zu können.

Messverfahren

Neben den Verfahren, Checklisten- bzw. papierbasiert und auf Eintrittswahrscheinlichkeiten beruhend, die Sicherheit zu messen, existiert mit dem OSSTMM ein operativer Sicherheitstest. Wichtig bei diesem Messverfahren ist, dass es auf dem Grundsatz der „Perfect Security“ aufbaut. Die „Perfekte Sicherheit“ stellt ein individuelles Maß an Subjektivität, vor dem Hintergrund der eigenen Anforderungen der definierten perfekten Sicherheit, dar. Somit fordert das OSSTMM, sich von pauschalen Konzepten zu verabschieden und vielmehr zu hinterfragen, welche Sicherheit ein Unternehmen für seine Geschäftspolitik dediziert benötigt.

Dabei liegt dem OSSTMM ein Vier-Punkte-Prozess zugrunde, der nicht nur das Zielsystem selbst untersucht, sondern mit hoher Genauigkeit und Gründlichkeit insbesondere die direkte Umgebung des Zielsystems untersucht, um über diese Vektoren die Kompromittierung der notwendigen Sicherheitsziele zu überprüfen.

Der RAV dient somit der Wirksamkeitskontrolle von Sicherheitsmaßnahmen und ihrer Bemessung.

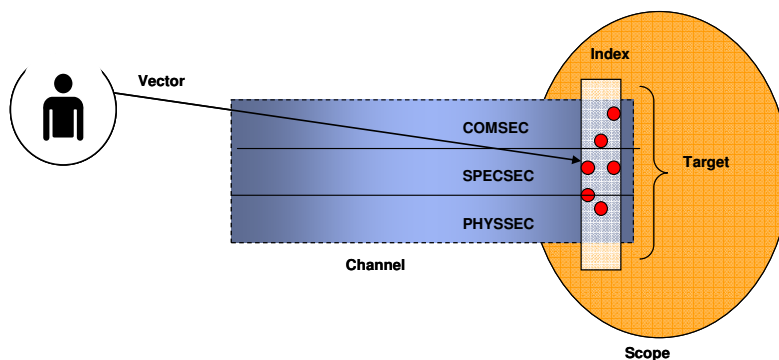


Abbildung 4 4-Punkt-Prozess

Dabei ist bedeutsam zu erkennen, dass das OSSTMM technisch tiefgehend und manuell verifizierend auf eben diese Wirksamkeit der sicherheitstechnischen Gegenmaßnahmen hin prüft. Dies beinhaltet auch einen im deutschsprachigen Raum begrifflich häufiger verwendeten Penetrationstest, nur, dass ein OSSTMM-konformer Sicherheitstest weitergehend ist.



Abbildung 5 Prüfung der Wirkweise

Test: Wie – Wer – Was?

So werden bei einem solchen OSSTMM-konformen technischen Sicherheitsaudit drei Dimensionen gemessen:

- Operative Sicherheit
- Sicherheitsmaßnahmen (Loss Controls)
- Sicherheitslücken (Security Limitations)

Dabei wird für die Feststellung der operativen Sicherheit die gegebene Durchlässigkeit, aufgegliedert in Sichtbarkeiten (Visibilities), Zugängen (Accesses) und Vertrauensstellungen (Trusts) als „Porosity“ gemessen. Für diese optimalerweise geschäftsgerichteten, operativen Sicherheit-Designs, werden die implementierten Sicherheitsmaßnahmen, die

dem Sicherheitsverlust entgegenwirken sollen (Loss Controls), ebenso gemessen wie die Sicherheitsbeschränkungen, die im Audit manuell verifiziert werden müssen.

In einer Formelfunktion kombiniert, ergibt dies den aktuellen Sicherheitswert zwischen Null und Hundert.

Testleistungen

Das OSSTMM verfügt über 17 Module, welche in einem standardisierten Vorgehensmodell angewendet und durchgeführt werden.

Neben den durch die technisch tiefgehenden Tests aufzudeckenden aktuellen Sicherheitslücken, werden in einem OSSTMM-Audit auch die gegebene Compliance-Situation sowie die Anwendung von BestPractices und die Wirksamkeit von Sicherheitsmaßnahmen dargestellt. Der RAV-Wert spielt dabei für unterschiedliche, im Dialog mit dem überprüften Unternehmen erarbeiteten Frage- und Themenstellungen, einen Schwerpunkt. Hieraus können konkrete Empfehlungen, Maßnahmen und Aktionspläne abgeleitet werden, die dem Kunden sowohl im Abschlussbericht in textueller, als auch in einem Transfer-Workshop in medialer und kommunikativer Form dargestellt und diskutiert werden.

Kundennutzen

Der Kunde hat bei Anwendung eines OSSTMM-Sicherheitsaudits den Vorteil, dass er auf faktischer Grundlage das Investitionsvolumen für IT-Sicherheit gründlich bestimmen und steuern kann. Da in der Regel eine Priorisierung von Maßnahmen erfolgen muss, kann der RAV helfen, gemessen an Geschäftsanforderungen und den zu schützenden Assets und auf Grundlage von Geschäftsprozessen, Investitions- und Implementierungs-Entscheidungen zu priorisieren.

Ein weiterer Vorteil der RAV-Bemessung innerhalb eines OSSTMM-Audits ist, dass in Sicherheitskategorien gedacht werden kann, um z.B. Lösungen entsprechend bewerten zu können. Dies bedeutet eine Abkehr von Lösungen und Produkten, bis hin zu rationaleren Entscheidungen. Dies gilt in gleichem Umfang auch für die Optimierung von Sicherheit. Der RAV hilft, periodisch die Sicherheitsanstrengungen und ihre Verbesserungen zu vergleichen und einen Ratio zwischen dem Schutzniveau und den Instandhaltungskosten für IT-Sicherheit zu bilden.

Da der RAV die Effektivität von Schutzmaßnahmen im Hinblick auf die gegebene Porosität bestimmt, bemisst der RAV genau genommen nicht den Grad der Sicherheit, sondern den Grad der Unsicherheit.

Dies ist insbesondere für das bislang stets unter vielen und gewichtigen Annahmen mit unter Umständen voreingenommenen Werten betriebene Risikomanagement der IT, eine wesentliche Innovation und Hilfestellung.

Den Unternehmen, die ihre Informationssicherheit klar definiert und geregelt haben, z.B. auf der organisatorischen Ebene, bietet das OSSTMM die Möglichkeit, den Wirkungsgrad auf Basis einer unumstößlichen Faktenlage hinsichtlich des Sicherheitsniveaus zu bemessen.

Dies gilt insbesondere auch für den Unterstützungsgrad der IT für Geschäftsprozesse, woraus sich differenzierte Optimierungsvorteile ableiten lassen.

Fazit

OSSTMM macht aus IT-Sicherheit eine exakte Wissenschaft, mit der es möglich ist, Informationstechnologien faktisch zu bemessen, IT-Sicherheit wirtschaftlich zu planen und

die Geschäftsprozesse effektiv zu verbessern und hinsichtlich ihrer Sicherheit zu optimieren.

Wer IT-Sicherheit nicht misst, muss sich die Frage gefallen lassen, warum er von der Richtigkeit des Handelns überzeugt ist und wie er es pragmatisch verbessert. Denn letztlich gilt der alte Management-Grundsatz: Du kannst nicht managen, was du nicht misst!

Heiko Rudolph

adMERITia GmbH i. G.