



HEIKO RUDOLPH

Informationssicherheit intelligent steuern

Schwierigkeitsgrad:



Die Frage nach der Steuerung von Informationssicherheit (IS) ist in vielen Unternehmen und Behörden noch immer offen, erst recht, wenn es um eine pragmatische und angemessene Art und Weise geht.

In diesem Artikel soll ein Ansatz skizziert werden, wie mit Hilfe einer Sicherheitsmetrik, basierend auf einem offenen Teststandard namens „Open Source Security Testing Methodology Manual“ (OSSTMM) im Zusammenspiel mit standardkonformen Disziplinen zur Überwachung des festgelegten Sicherheitsniveaus die IS gesteuert werden kann. Dabei beschreibt er zunächst das gesamtheitliche Zusammenspiel und geht anschließend auf die unterstützende und verknüpfende Funktion von OSSTMM ein.

Diesem Ansatz liegen drei Grundsätze zugrunde:

- IS ist kein Selbstzweck sondern hat das Geschäftssystem zu schützen
- Das Informationseigentümer-Prinzip wird angewendet
- Die IS soll wirtschaftlich angemessen ausgerichtet werden

Dass IS kein Selbstzweck ist, sondern ausschließlich dafür zu sorgen hat, dass durch den Einsatz von Informations- und Kommunikationstechnologien (ITK) bei der Abbildung und Realisierung von Geschäftsprozessen und Service keine zusätzlichen operationellen Risiken entstehen, sollte selbstverständlich sein. Leider ist in der Realität ein anderes Bild zu beobachten. Unternehmen und Behörden tun sich noch immer schwer, IS in Ihren Unternehmenskulturen

sinnvoll zu etablieren. Einerseits verlaufen sich viele Organisationen aufgrund mangelnder „Leitsysteme“ für IS trotz guter Standards, wie zum Beispiel der ISO 2700x-Normenwelt. Solche Standards sind in der Regel sehr generisch, was sie auch sein müssen, um ihre Standardisierungsfunktion zu erfüllen. Problematisch wird es freilich bei der Adaptierung auf ein entsprechendes Geschäftssystem. Wobei häufig zu beobachten ist, dass die Erkenntnis darüber, was eigentlich als schützenswert in einer Organisation gilt, fehlt. Dies macht die korrekte Anwendung generischer Standards natürlich nicht einfacher, so dass alleine schon deswegen eine wirtschaftliche Angemessenheit häufig verfehlt wird.

Wirksamkeit vs. Existenz

Andererseits fehlt eine ganzheitliche Sicht auf die IS. Dies wird vor allem dort deutlich, wo die Verbindung zwischen der organisatorischen und der technischen Sicherheit fehlt. So existieren in Organisationen zwar zunehmend Regelungen, die IS betreffend, jedoch fehlt es an der Kontrollinstanz der Wirksamkeit derselben. Als Beispiel dient die Sicherheitsrichtlinie, welche einen Telnet-Zugang kategorisch verbietet, dieser aber existiert. Der Regelkreis zwischen Definition, Existenz und Wirksamkeit ist durchbrochen. Ein Dashboard zur Messung der eigenen (angemessenen) IS ist so gut, wie nie anzutreffen. Reports, wie beispielsweise die Anzahl der Virenangriffe taugen selbstverständlich nicht. Sie sind eher als

IN DIESEM ARTIKEL ERFAHREN SIE...

Am Beispiel eines standardbasierten Risk Assessment-Verfahrens, wie die Sicherheitsmetrik von OSSTMM hilft, Informationssicherheit zu messen, überwachen und zu steuern.

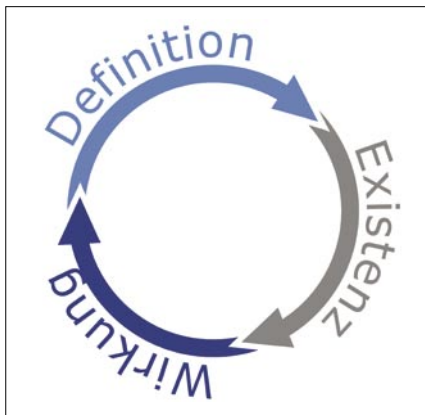


Abbildung 1: Definition-Existenz-Wirkungs-Regelkreis

verzweifelter Versuch zu werten, die IS in Zahlen abzubilden. Eine Aussage über das Schutzniveau treffen sie nicht. Und schon gar nicht über das angemessene.

Bei der Fragestellung, was eigentlich zu schützen und welche Informationen und Daten, wie (geschäfts)kritisch sind, kann der Grundsatz der Informationseigentümerschaft helfen. Leider ist in der Praxis viel zu häufig zu beobachten, dass die Fachabteilungen noch nicht verantwortlich für Ihre Daten und Informationen sowie Prozesse sind. Letztlich können aber nur sie die Risiken anhand von Bedrohungslagen einschätzen. Dies kann weder eine IT-Abteilung noch ein Security Competence Center. Erstaunlicherweise gehen allerdings viele Fachabteilungen davon

aus, dass ihre Daten schlichtweg sicher sind und formulieren quasi implizit die Anforderung. Dieser kann die IT nicht nachkommen, weil sie ja nicht weiß, was wie stark zu schützen ist. Dieses Dilemma gilt es freilich über die Informationseigentümerschaft aufzulösen, indem die Fachabteilung kompromisslos verantwortlich ist für die von Ihnen produzierten und verwalteten Daten, Informationen und Prozesse.

Wenn dieser Zustand erreicht ist, kann eine angemessene IS eingeführt und gesteuert werden.

Steuerung der IS

Betrachtet man die Organisation von IS anhand des oben genannten ISO-Standards in der Norm 27001 (Informationssicherheits-Managementsystem; ISMS) lässt sich feststellen, dass einzelne ISO-Abschnitte sich stärker mit der Ausgestaltung der organisatorischen Sicherheit beschäftigen, wie z. B. der Security Policy, der IS-Organisation, dem Asset Management und dem Human Resources Security. Weitere Abschnitte befassen sich im Detail mit Controls, wohinter sich Schutzmechanismen definieren für physische und Umgebungssicherheit, Kommunikations- und Operationsmanagement und Zugangskontrolle oder der Beschaffung,

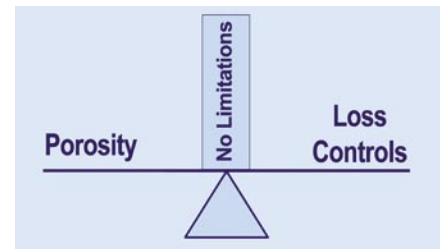


Abbildung 3: Balance-Konzept OSSTMM

Entwicklung und Instandhaltung von Informationssystemen. Andere Abschnitte, wie das Information Security Incident Management, das Business Continuity Management und die Compliance-Abschnitte legen Maßnahmen zur Überwachung und Steuerung des Sicherheitsniveaus fest. Wir wollen uns auf diese Abschnitte fokussieren und aufzeigen, wie mit Hilfe einer offenen Methode eine Sicherheitsmetrik adaptiert werden kann, um auf Grundlage oben genannter Grundsätze die IS einer Organisation gesamtheitlich zu steuern. Das Zusammenspiel wird auch in der Abbildung 2 deutlich.

Wie in der Abbildung verdeutlicht, konzentrieren wir uns auf die folgenden Disziplinen:

- Vulnerability Management,
- Security Incident Event Monitoring (SIEM),
- Compliance Management,
- Penetrationstests.

Diese Disziplinen bilden die erste Schicht eines Steuerungsinstrumentariums für IS.

In der zweiten Schicht sehen wir im Kern eine Bewertungsebene, in der auf Basis der Sicherheitsmetrik von OSSTMM jeweilige Aspekte quantifiziert und qualifiziert werden.

Hierauf setzt eine dritte Schicht auf, bestehend aus:

- Business Continuity Management (BCM),
- Risikomanagement,
- Business Process Management (BPM),
- Information Security Management System.

Hierüber erschließt sich das Geschäftsmodell mitsamt Strategie und

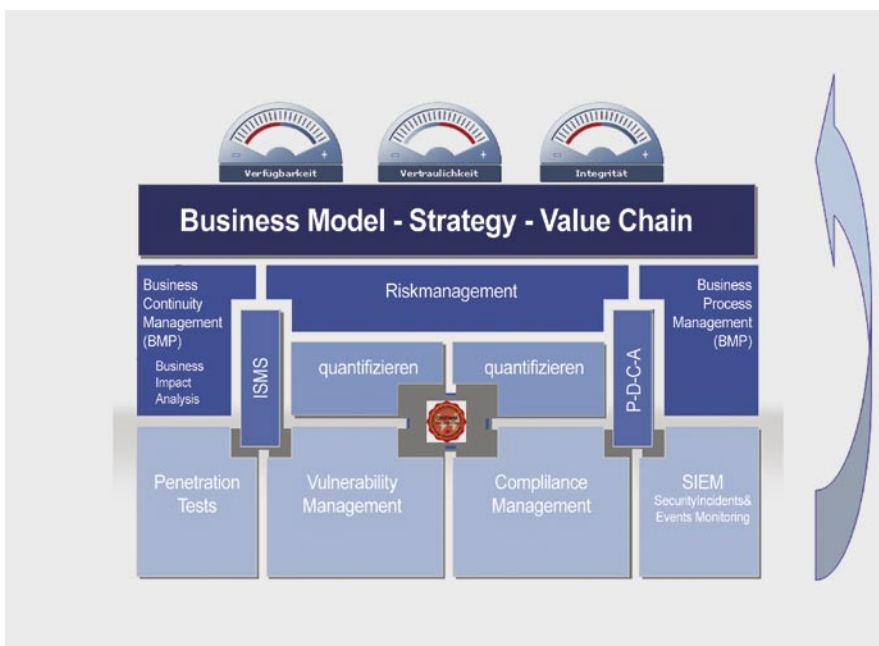


Abbildung 2: Ganzheitliche IS-Steuerung

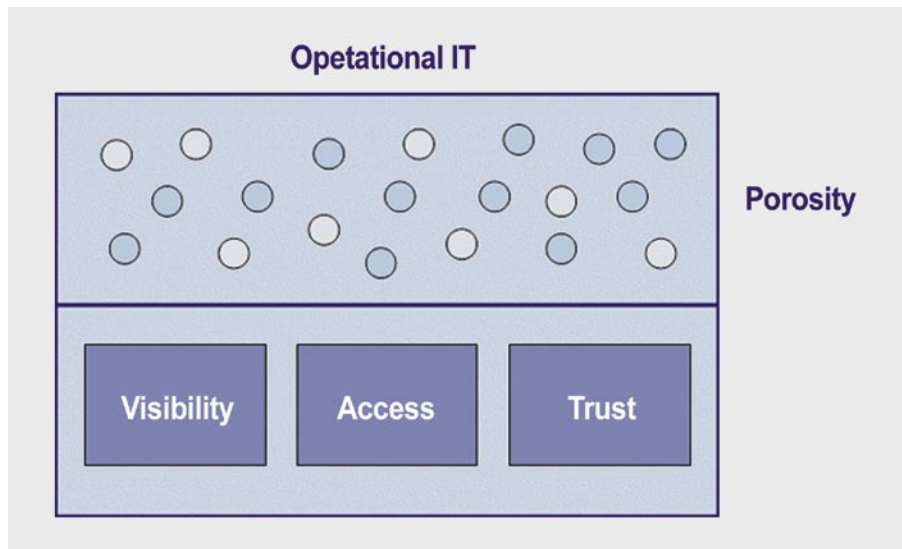


Abbildung 4: Porosität eines Zielbereiches

Wertschöpfungskette, in der das gesamte Geschäftssystem abgebildet wird.

Basierend hierauf wird ein Dashboard angelegt, welches in aggregierter Form die jeweiligen Zustände des faktischen Sicherheitsniveaus visualisiert.

Nachfolgend soll das Zusammenwirken der Disziplinen aufgezeigt werden. Die einzelnen Anforderungen aus der ISO 27001 zur Überwachung und Steuerung des (angemessenen) Sicherheitsniveaus können selbstverständlich mit unterschiedlichen Produkten, Tools und Suiten erledigt werden. Auch wenn die Herstellerseite dies nutzt, um ihre Produkte im Markt zu platzieren und mit Hilfe der Disziplinenbegriffe vermarktet, ist damit noch lange kein angemessenes Sicherheitsniveau erreicht. In allererster Linie fehlt die Abbildung der Sicherheit auf das Geschäftssystem.

Natürlich müsste das Geschäftsmodell die Vorgaben für eine angemessene IS liefern. Dies ist in der Praxis leider nicht ausgeprägt. Das Management ist in der Regel zu wenig auf operationelle Risiken sensibilisiert, welche aus dem Einsatz von ITK-Technologien herrühren. Insofern kann auch Bottom-Up verfahren werden, indem die Überwachungsdisziplinen quantifiziert und qualifiziert werden und über ein Risikomanagement und Kontinuitätsmanagement sowie gegebenenfalls über ein Business-Prozessmanagement über die Strategie

an Vorgaben gekoppelt werden. Dies entspricht gleichzeitig auch dem PDCA-Regelkreis, welches dem ISMS der ISO 27001 zugrunde liegt.

Grundsätzliche Idee ist also, dass die jeweiligen Aspekte der Überwachungsdisziplinen so quantifiziert werden, dass BCM, Risikomanagement und BPM entscheidungsrelevante Aussagen treffen können, um Vorgaben hieraus abzuleiten. Diese Vorgaben können sodann sicherheitsmetrisch überwacht und gesteuert und in einem Dashboard visualisiert werden.

Dabei ist wichtig, die beiden äußersten Flanken, bestehend aus BCM und BPM als tragende Säulen zu erkennen. Die ISO 27001 sowie weitere Standards, wie z. B. die BSI-100-Normenreihe, empfehlen stets, die IS an den Geschäftsprozessen auszurichten. Diese werden im Rahmen des BPM verwaltet und gesteuert. Nicht zuletzt durch die umwälzende Einführung von Service Oriented Architectures (SOA) wird dies von zunehmender Bedeutung. Dabei ist zu beobachten, dass sich Geschäftsprozesse in Services integrieren, welche in den verschiedenen Schichten der SOA-Architekturen angesiedelt sind. Durch die Bündelung unterschiedlicher Applikationen zu Services ist der Geschäftsprozess bzw. der Service der einzige sinnvolle Pfad, um Risiken für eine Organisation zu bewerten. Diese Bewertung erfolgt im Risikomanagement mittels Risikoakzeptanzverfahren, welche sich wiederum der sicherheitsmetrischen

Bemessung von OSSTMM bedienen und auf die Sicherheitsmetrikerwerte zurückgreifen. Ein Risikomanagement stellt zumindest nach deutschem Recht auf ein internes Kontrollsystem (IKS) ab. Meint man es ernst damit, wird man sich zukünftig wohl kaum der bislang üblichen tendenziell eher Checklisten-basierten Vorgehensweise weiter bedienen können.

Auch das BCM stellt den Geschäftsprozess in den Fokus seiner Betrachtungen. In der Business Impact Analysis (BIA) werden Folgeschäden abgeschätzt. Eine solche Folgeschäden-Abschätzung kann hervorragend auf faktischem Niveau mittels der OSSTMM-Sicherheitsmetrik durchgeführt werden.

Risk Assessment Value für Risk Assessment NIST SP 800-30

Dabei kann das Risikomanagement wie auch das BCM jeweils auf die faktischen Grundlagen, welche in der sicherheitsmetrischen Bemessung von OSSTMM herausgearbeitet wurden, zurückgreifen. Das OSSTMM und seine Sicherheitsmetrik basiert auf einem Balance-Konzept, welches in Abbildung 3 nochmals veranschaulicht wird.

Das Balance-Konzept besteht im Wesentlichen aus drei Elementen:

- Porosität,
- Controls,
- Limitations (Sicherheitslücken).

Die Porosität ergibt sich aus der jeweiligen Kommunikationsbeziehung innerhalb eines gewissen Scopes aus Visibilities (z. B. Live Hosts, IPs, Systeme, Gebäude o. ä.), Access (Dienste) und Trusts (Vertrauensstellungen). Der Begriff der Porosität bezeichnet in der Nomenklatur des OSSTMM die Durchlässigkeit eines Zielbereiches, was Abbildung 4 gut verdeutlicht. Insofern charakterisiert sie auf einfache Weise einen Zielbereich.

Ein Zielbereich kann ein einzelnes System oder ein IT-Verbund sein. Es kann sich aber auch um einen Geschäftsprozess handeln, der durch unterschiedliche Systemen und Applikationen abgebildet wird. Die Durchlässigkeit eines Zielbereiches wird

nun mit Loss Controls ausgeglichen. Loss Controls sind Schutz- oder Sicherheitsmechanismen, wie z. B. Authentifizierung, Alarmer, Integritätsschutz etc. Das OSSTMM kennt zehn Loss Controls gegliedert in zwei Kategorien. Die insgesamt zehn Schutzklassen lassen sich in Mappings gegen sämtliche Sicherheitsstandards, wie beispielsweise ISO 27001, BSI-100-x bzw. Grundschutzkatalog, CoBIT, COSO, PCI DSS usw. einordnen. Damit ist man nicht nur sehr flexibel, weil man jeden Standard, nachdem Organisationen ihre IS ausgerichtet haben, umsetzen kann. Es wird auch eine Verbindungsschicht zwischen der organisatorischen und der technischen Sicherheit geschaffen. Eine solche hilft, den Umsetzungsgrad der Richtlinien transparent und Dank der Sicherheitsmetrik auch quantifiziert sichtbar zu machen.

Dabei werden sie im Kosten-Nutzen-Verhältnis auf Grundlage eines Risikoakzeptanzverfahrens über die Sicherheitsmetrik optimal ausbalanciert. So machen selten alle Schutzmechanismen Sinn oder sind überhaupt technisch möglich. Dementsprechend müssen diese angepasst werden, was sich in einem Key Performance Indicator (KPI) widerspiegelt.

Das „Zünglein an der Waage“ sind die Limitations, welche die Sicherheitslücken darstellen. Wie in Abbildung 5 erkennbar, kategorisiert OSSTMM sie und grenzt sie ebenso eindeutig wie objektiv voneinander

ab. Hierdurch wird ein Willkürfaktor in der Bewertung ausgeschlossen, was ein Herzstück für eine faktische Risikobewertung ist.

Ordnet man nun die einzelnen Überwachungsdisziplinen dem OSSTMM zu, so können Penetrationstests sehr effektiv mit OSSTMM durchgeführt werden, wobei der OSSTMM-Testkatalog zur Anwendung kommt. Das Vulnerability Management kann mit Hilfe der Sicherheitsmetrik von OSSTMM jede Anfälligkeit in eine entsprechende Security Limitation umwandeln und somit in einen sicherheitsmetrischen Wert ausgeben.

Compliance Management

Für das Compliance Management dreht OSSTMM den Spieß um: Anders als am Markt platzierte Werkzeuge agiert das OSSTMM „Finding-basiert“. Dies bedeutet, dass basierend auf einer Auffälligkeit (Finding) geprüft wird, ob Verstöße gegen Gesetze, regulatorische Auflagen, interne Richtlinien und Prozesse vorliegen. Je nach Ausprägung des Compliance Management-Tools in der Überwachungsschicht können diese kombiniert werden.

Das Security Incident and Event Monitoring (SIEM) kann wiederum über die Porosität, die Loss Controls und / oder die Security Limitations dargestellt werden. So lässt sich jedes Incident oder Event mindestens einem der drei Bereiche Visibility, Access und/oder Trust zuordnen. Die sie ausbalancierenden

Loss Controls sind durch einen Incident oder Event jeweils betroffen, sei es dass ein Control nicht so wirkt, wie vorgesehen oder fehlt, weil es im initialen Security Design nicht hinreichend berücksichtigt wurde. Letztlich lässt sich eine Auffälligkeit oder ein Ereignis aber häufig auch einer Sicherheitslücke zuordnen. Umgekehrt lässt sich dieser Weg natürlich auch beschreiten, denn OSSTMM kann über seine Balanceelemente auch Incidents oder Events darstellen.

Mit Hilfe von automatisierten OSSTMM-Tests, bzw. Test-Modulen können ersatzweise auch das Vulnerability Management entfallen, sollte dies nicht etabliert sein.

Mit Hilfe der Sicherheitsmetrik können nun Veränderungen im Zielbereich z. B. an der Durchlässigkeit durch neu hinzugekommene Dienste oder Trusts oder Server ebenso quantifiziert werden, wie implementierte oder im Rahmen von Change Management entfallene Controls. Für das Risikomanagement oder das Business Continuity Management nebst Business Impact Analyses werden diese sicherheitsmetrisch herausgearbeiteten Aspekte nun qualifiziert, so dass Sie in Risikoakzeptanzverfahren übernommen werden können.

Anhand des Risikomanagements bzw. der Risikoeinschätzung soll nun ein beispielhaftes Zusammenspiel aufgezeigt werden. Als Grundlage hierzu dient der Standard NIST SP 800-30 „Risk Management Guide for Information Systems“ der US-amerikanischen Behörde National Institute for Standards and Technology (NIST). Das Risikobewertungsverfahren „Risk Assessment Methodology Flowchart“ geht aus Abbildung 6 hervor.

Der sehr generische und theoretisch anmutende NIST-Standard wird im Folgenden mit Unterstützung des OSSTMM und seiner Sicherheitsmetrik durchlaufen, wobei Abweichungen von der reinen NIST-Lehre auf den praxiserprobten Ansatz zurückzuführen sind.

Der initiale Schritt der Systemcharakterisierung geht einher mit der Abgrenzung des Zielbereiches. Im gleichen Schritt kann für den Zielbereich die Porosität ermittelt werden, so dass ein wesentliches Element der

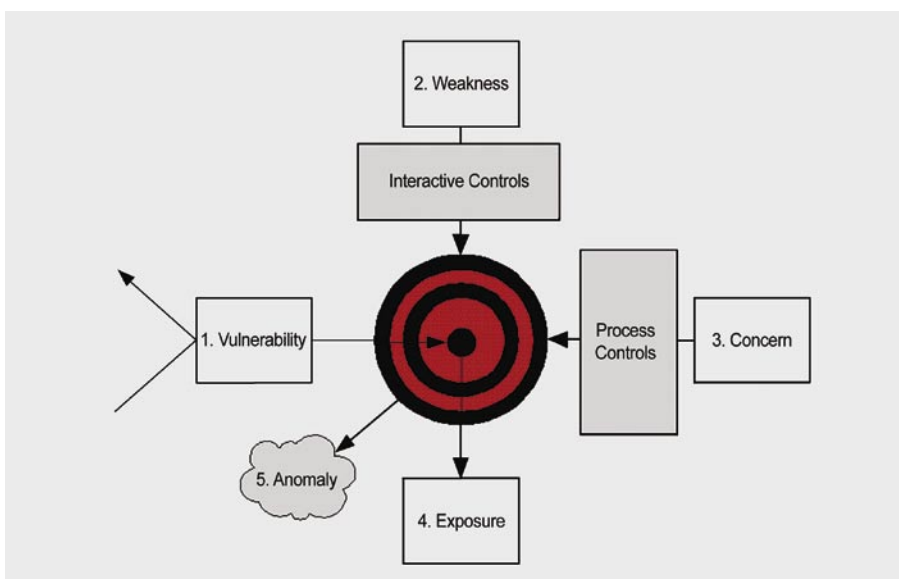


Abbildung 5: Security Limitations

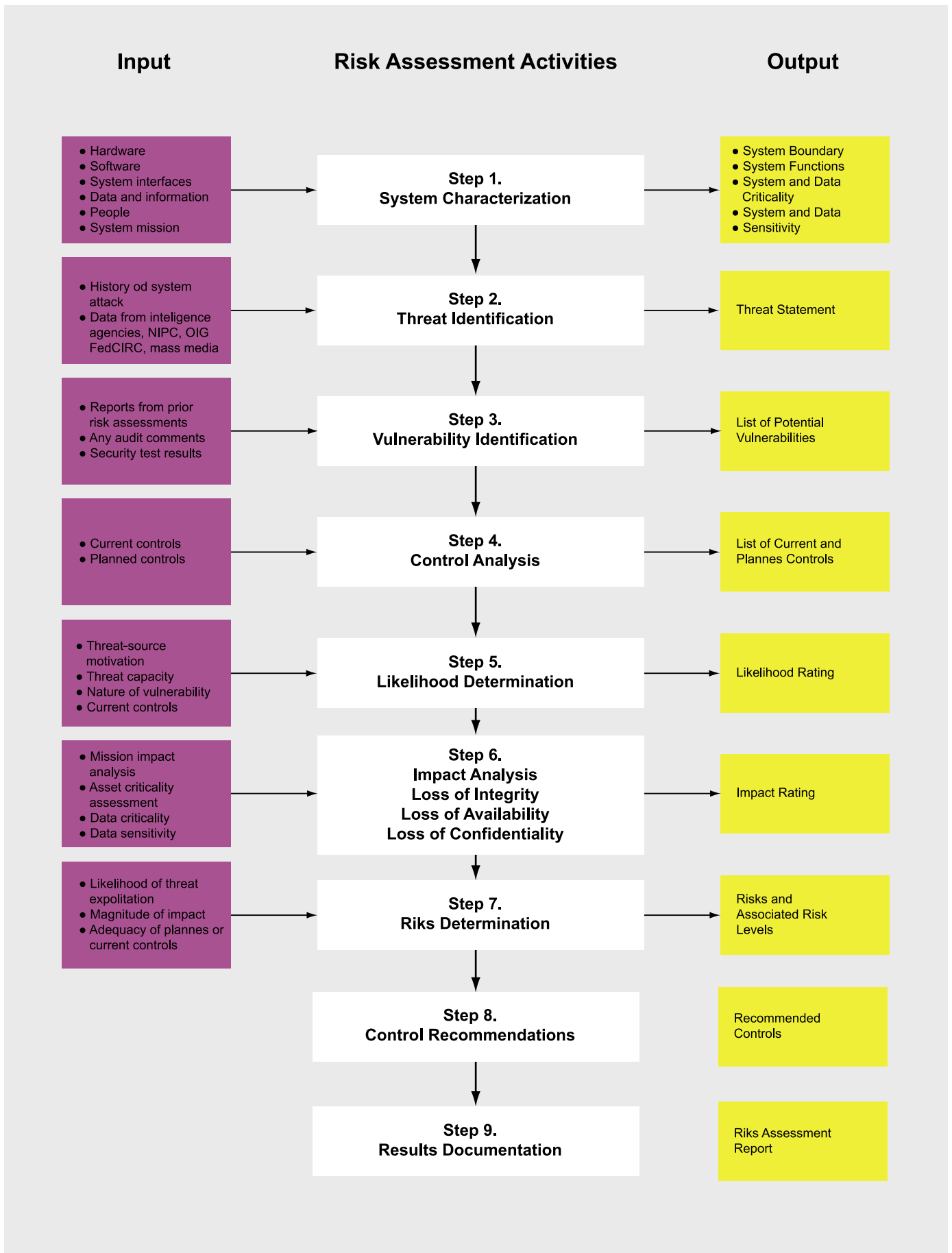


Abbildung 6: Risk Assessment Methodology Flowchart NIST SP 800-30

Sicherheitsmetrik schnell zur Verfügung steht. Dabei werden die einzelnen Kommunikationsbeziehungen autorisiert und sichergestellt, dass sie gerechtfertigt sind.

Im zweiten Schritt wird die Bedrohungslage identifiziert, wozu Vektoren aus den unterschiedlichen Bedrohungsperspektiven auf den Zielbereich definiert werden. Dieser Schritt bedient sich nicht der Sicherheitsmetrik, ist aber hinsichtlich der grundsätzlichen Einschätzung von elementarer Bedeutung, weil die Vektoren auf die schützenswerten Güter, die sogenannten Assets gebildet werden. So wird durch diesen Schritt transparent, was es eigentlich zu schützen gilt. Hier kommt bereits erstmals das Prinzip der Informationseigentümerschaft zum Tragen.

Schritt drei beschäftigt sich mit der Identifizierung von Anfälligkeiten des Zielbereiches. Existiert der Zielbereich bereits, kann ein technisches OSSTMM-Audit hierauf angewendet werden, um die faktisch bestehenden Sicherheitslücken, die Security Limitations zu bestimmen. Sprechen Gründe gegen ein solches verifizierendes Verfahren, beispielsweise, weil der Zielbereich noch nicht aufgebaut ist, arbeitet man mit tendenziellen Sicherheitslücken. Allerdings ist hierbei wichtig zu verstehen, dass solche nur die halbe Wahrheit sagen, denn man würde lediglich auf bereits bekannte Anfälligkeiten aus öffentlich verfügbaren Vulnerability-Datenbanken oder allgemeine Erfahrungswerten zurückgreifen. Ebenfalls würden Anomalien und sogenannte „Zero Day Exploits“ unter den Tisch fallen, was unfraglich nicht im Sinne einer vollständigen Risikobewertung wäre. Unabhängig vom Bestimmungsweg, werden die Limitations gemäß OSSTMM kategorisiert, was im gleichen Zug zu sicherheitsmetrischen Werten führt. Somit ist das zweite Element der Sicherheitsmetrik errechnet.

Im nächsten, den vierten Schritt beschäftigt man sich mit der Analyse der Controls. Begrifflich sind die Controls den Loss Controls von OSSTMM gleichgestellt. Dem Balancekonzept von OSSTMM folgend gleichen die Loss Controls die Porosität aus und sichern somit den Zielbereich ab. Der Grad der Absicherung

kann dabei feingliedrig auf das erforderliche, nämlich angemessene Sicherheitsniveau angepasst werden. Die implementierten oder geplanten Sicherheitsmaßnahmen werden über Mappings den Loss Controls von OSSTMM zugeordnet. Gleichzeitig werden sie sicherheitsmetrisch bemessen, womit das dritte Element der Metrik bestimmt ist. Sofern in dem NIST SP 800-30 von einer Analyse der Controls spricht, kann dies vollumfänglich mit OSSTMM erledigt werden. Aber OSSTMM geht noch einen Schritt weiter, wenn die Controls den zu akzeptierenden Risiken angepasst werden.

Sicherheitsmetrisch bemessen wird jedes Element durch seine Zählung. Der gezählte Wert fließt in die logarithmische RAV-Formel ein. Als Ergebnis wirft die Metrik einen Gesamtwert, den RAV-Wert aus. Dieser kann einen Key Performance Indicator (KPI) repräsentieren. Diese können zu verschiedenen Zwecken Soll-Ist-Vergleichen unterzogen werden, wobei hieraus hergeleitete Abweichungen Handlungsbedarfe aufzeigen können. Damit können Evaluationen von Technologien, Architekturen, Security Designs, Lösungen und Produkten ebenso auf metrischer Basis durchgeführt werden, wie der Ist-Zustand von Zielbereichen gemessen, überwacht und gesteuert werden. Zwar handelt es sich bei den RAV-Werten um aggregierte Werte, jedoch lassen diese sich durch Drill-Down-Effekte bis auf die kleinste Einheit auf Ebene der Kommunikationsbeziehung herunterbrechen und jederzeit berichts-fähig und visualisiert aufbereiten.

Doch zurück zum Risk Assessment auf Grundlage des NIST-Standards. Durch eine vergleichende Analyse der Werte können die Controls im Hinblick auf das vertretbare Risiko definiert werden. Hierbei können auch Kosten-Nutzen-Effekte berücksichtigt werden, da Controls zu einem gewissen Teil Ausgaben, Investitionen und/oder Kosten verursachen. Dies kommt gemäß der NIST-Theorie erst im letzten Schritt, kann aber hier schon eingebunden werden, was Effektivitätsvorteile beinhaltet.

Der fünfte und sechste Schritt kann zusammengefasst werden. In Durchgang fünf erfolgt eine Wahrscheinlichkeitsbestimmung der einzelnen Bedrohungen,

welche sich aus den Sicherheitsmetrik elementen Porosität, Loss Controls und (etwaig tendenziellen) Security Limitations herleiten lassen. Ihnen werden in einer Matrix die aus dem sechsten Schritt, der Business Impact Analysis, ermittelten Bedrohungsarten gegenübergestellt, welche jeweils mit Wahrscheinlichkeitskategorien belegt werden. Hieraus kann das gesamtheitliche Gefahrenpotenzial je Bedrohung abgeleitet werden. Über die einzuschätzende Wahrscheinlichkeit kann entsprechend priorisiert werden.

Nun ist durch die Wahrscheinlichkeitsbestimmung der Willkür erneut Tür und Tor der subjektiven Einschätzung geöffnet. Wie hilft aber nun die Sicherheitsmetrik dabei? In erster Linie eröffnet sie Dank ihrer klaren Strukturierung und gleichzeitig hohem Methodikanteil die Möglichkeit, die Bedrohungen transparent zu ermitteln und darzustellen. Als zweiten aber nicht minder wichtigen Effekt unterstützt sie dabei, den Grad der Wirksamkeit von Controls sowohl objektiv als auch quantifiziert darzustellen, was ein bedeutender Fortschritt gegenüber der bislang auf Annahmen basierenden Verfahrensweise ist. Letztendlich können Kosten-Nutzen-Evaluierungen von Schutzmechanismen im Hinblick auf vertretbare Risiken metrisch abgebildet und somit versachlicht werden.

Im vorletzten Schritt müssen die Risiken bestimmt werden. Dazu werden die vorhandenen differenzierten Risklevel und entsprechenden sicherheitsmetrischen RAV-Werten beigeordnet.

Auf dieser Grundlage werden der reinen Lehre folgend im letzten Schritt die Controls empfohlen. Wie oben bereits dargelegt, kann dieser Schritt mit OSSTMM auch früher eingebunden und so mehr Effektivität erzielt werden.

Fazit

Zwar ist die Sicherheitsmetrik von OSSTMM kein Heilsbringer oder gar ein Allheilmittel. Vor dem Hintergrund stark annahmebasierter Verfahren ist sie jedoch ein gutes Mittel, um faktisch, objektiv und quantifiziert die einzelnen Sicherheitsdisziplinen effektiver, als bislang möglich auszurichten und die IS insgesamt zu überwachen und zu steuern.