

Einsatz von Metriken beim Security Monitoring

IT-Sicherheit messbar machen

09.01.2008 | Autor: Lothar Lochmaier

Rund 80 Prozent der Sicherheitsrisiken im Unternehmen liegen unterhalb der Wasseroberfläche. Deshalb ist es oft nur eine Frage der Zeit, bis das Unternehmen selbst zum Notfall wird. Dennoch fällt es den Spezialisten ausgesprochen schwer, die für sie relevanten Risiken konkret zu messen. Metriken können dazu eine Hilfestellung gegeben, sofern sie an der richtigen Stelle ansetzen.

Rein mathematische Modelle eignen sich als Metriken in der IT-Security nur bedingt. Denn sie haben sich in der Praxis häufig als eine Art „Kaffeesatzleserei“ erwiesen. „Oftmals bleibt bereits unklar, was die Unternehmen konkret messen bzw. steuern wollen“, gibt Stefan Strobel, Geschäftsführer beim IT-Sicherheitsspezialisten Cirosec GmbH zu bedenken.

Der Experte macht dafür vor allem die große Verwirrung anhand unscharf definierter Begrifflichkeiten verantwortlich. Oftmals verwechselten die Unternehmen Äpfel und Birnen, etwa indem sie so heterogene Elemente wie Bewertung, Audit, Penetrationstest, Risikoanalyse, Metrik und Kennzahlen durcheinander wirbelten.

So bezeichnet der Begriff Metrik (griechisch: Messung) nach allgemeiner Definition ein System von Kennzahlen oder ein Verfahren zur Messung einer quantifizierbaren Größe. Jedoch sei nicht alles, was gezählt werden könne, messbar, bzw. nicht alles, was gezählt werden könne, zähle überhaupt, beschreibt Stefan Strobel in Anlehnung an Albert Einstein die schwierige Gratwanderung der IT-Sicherheitsspezialisten.

In der Praxis macht es zudem einen großen Unterschied aus, ob es sich bei der Bewertung der IT-Sicherheit bzw. insbesondere der Verfügbarkeit etwa um den systembedingten Ausfall bei einer Flugreservierung oder einem Online-Broker handelt, oder aber um ein Unternehmen, das weit weniger kritische Prozesse im Internet betreut.

Welche Zielsysteme dementsprechend dem höchsten Schutzbedarf unterliegen, ist deshalb alles andere als simpel festzulegen. Eine grundlegend falsche Annahme wäre es bereits, Sicherheitsmaßnahmen als Maßnahmen für mehr Umsatz zu betrachten. Auch wenn IT-Sicherheit vielfach als „Business Enabler“ dargestellt wird, so werden die Maßnahmen doch in erster Linie zur Kostenreduktion ergriffen. Aber auch das kann schon der falsche Ansatz an. Stefan Strobel sieht das konkrete Bewerten der IT-Sicherheit nur dann als Erfolg versprechend an, wenn dem eine permanente Risikoanalyse voraus gehe und keine einfache Eventkorrelation. „Ein schlechtes Beispiel wäre etwa, die Effektivität einer Firewall nur danach zu messen, wie oft die Regeln getriggert worden sind“, gibt der Experte zu bedenken.

Relevante Kennzahlen statt plumper Eventkorrelation

Um aus einem allzu grobmaschig gestrickten Betrachtungsmuster heraus zu kommen, greifen Unternehmen jetzt auf Kennzahlensysteme zurück. Diese stammen aus der Welt des betriebswirtschaftlichen Controllings,



cirosec GmbH
Edisonstraße 21
74076 Heilbronn
Tel: 07131 / 59455-0
Fax: 07131 / 59455-99
info@cirosec.de
www.cirosec.de

bergen aber ebenso wie die einfache Eventkorrelation das Risiko der Kaffeesatzleserei in sich. Denn Kennzahlen in der IT überhaupt zu messen, mache nur dann Sinn, wenn sich Ist- und Soll-Werte sinnvoll vergleichen bzw. bewerten ließen, bekräftigt Stefan Stroble.

„Die meisten Kennzahlen sind jedoch gar nicht mess- und steuerbar“, so der Experte weiter. Dennoch stelle das Bewerten der IT-Sicherheit mit Hilfe von Metriken ein sinnvolles Unterfangen dar, sofern die Zahlenwerke sich nicht wie beim klassischen Controlling anfühlten. Denn nur allzu häufig erweisen sich simple gestrickte Berechnungen eines „Security-Return-on-Invests“ (ROI) als Stolperstein.

Je differenzierter sich die Verantwortlichen im Unternehmen mit Ausfallszenarien und dem reibungslosen Betrieb und deren Abhängigkeiten auseinander setzen, umso genauer fällt die Prognose im Laufe der Zeit aus. Dazu gehört auch die Erforschung der Zusammenhänge und Ursachen. Kurzum: Ein einfaches Produkt aus Eintrittswahrscheinlichkeit mal Schadenshöhe ist Kaffeesatzleserei.

Experten konstatieren aufgrund dem meist vorherrschenden und durchaus verständlichen „Ad-hoc-Prozedere“ erhebliche Handlungsdefizite bei den Unternehmen. Oftmals überschätzen die Spezialisten die Bedeutung der IT-Systeme ohne konkrete Berechnungen. Das Bauchgefühl kann genauso trügerisch sein wie die allzu simpel gestrickte Mathematik. Nicht selten führt auch die Eskalation von kleineren Ausfällen oder Unterbrechungen an den Vorstand zu dem allgemeinen Verständnis, dass ein Ausfall nicht akzeptabel sei.

Konkret drückt sich diese ‚falsche‘ Annahme durch zu kurze Wiederherstellungszeiten (Recovery Time Objective) aus. Jede Verkleinerung der RTO führt jedoch zu einem unproportional hohen Anstieg der Kosten für Ersatzsysteme. Dies wiederum führt zu erheblichen Fehlinvestitionen, die an anderer Stelle fehlen. Der Grat zwischen über- und unterdimensionierter Prävention dabei ist äußerst schmal.

Ein zentraler Fehler ist die Entkopplung von Business und IT: Letztere läuft Gefahr, die Anforderungen in aller Regel vollkommen überhöht abzubilden. Die Folge besteht etwa in einem sehr aufwändigen und detailreich gestalteten Disaster-Recovery-Konzept, das aufgrund seiner hohen Kosten vom Business abgelehnt wird. Oftmals starten die Unternehmen daraufhin einen meist nicht sehr erfolgreichen zweiten Anlauf mit erniedrigten Anforderungen.

Externe Dienstleister versuchen dem entgegen zu wirken, indem sie deutlich machen, was der Kunde von einer Security ROI-Betrachtung erwarten kann und welche Ansätze nur eine Scheinsicherheit vermitteln. Falls die dann abgeschätzten Kosten aber weiterhin vom Business nicht mitgetragen werden, sind alle Beteiligten so frustriert, so dass die Übung schon zu Beginn gleich wieder einschläft.

Nur relevante Business-Prozesse in die Bewertung einfließen lassen

Deshalb gilt es vor der Definition unter Umständen von der unternehmerischen Realität völlig los gelöster Metriken die richtigen

Fragen beim Security-Management zu adressieren, und zwar mit Blick auf

den passenden konzeptionellen Ansatz einer internen Bewertung. Wie lange etwa darf das betreffende System ausfallen, wie lange dauert der Wiederanlauf? Bei der „Recovery Time Objective“ handelt es sich um die Zeit, die vom Zeitpunkt des Schadens bis zur vollständigen Wiederherstellung der EDV-Systeme vergehen darf. Es gilt dabei die so weit es geht objektiv als wichtig erkannten Risiken zu fokussieren.

Danach beginnt die Ermittlung des individuellen unternehmerischen Risikos. Wie konsistent ist der Datenbestand, wie hoch ist der Datenverlust, der in Kauf genommen werden kann? Dabei handelt es sich um die möglichst präzise Ermittlung des Zeitpunkts, wann und wie oft etwa die Datensicherung auf den unterschiedlichen Ebenen erfolgen soll, das heißt, wie viele Daten bzw. Transaktionen zwischen den einzelnen Sicherungen verloren gehen können. Neben diesen eher grundsätzlichen Fragestellungen hilft eine klare Vision der einzelnen Kostenblöcke, die sich in bezifferbare, schätzbare und nicht-bezifferbare Kosten untergliedern lassen.

Lösen Metriken das Problem oder schaffen sie nur neue Stolpersteine?

Als die größte operative Herausforderung beim Anlegen von Metriken im Bereich des Security Monitorings sieht Matthias Rosche, Mitglied der Geschäftsleitung bei der Integralis GmbH, die Vielzahl an protokollierten Ereignissen. Etwa 20 neue Schwachstellen ergeben sich täglich, glaubt man der Statistik von Organisation wie der cert.org. Der Experte sieht vor allem in der Norm ISO 17799 eine sinnvolle Ausgangsbasis, um mit dem nachhaltigen Security Monitoring einzusetzen.

Metriken stellten aber nur einen Bruchteil dessen dar, was auf der Aufgabenliste stehe. So müsse die Korrelation nicht nur das simple Logging umfassen, sondern auch Aspekte wie die Revisionsicherheit und Compliance einbeziehen. „Die Metriken müssen gegenüber dem klassischen Vorfallmanagement fundierte Trendaussagen zum Status Quo ermöglichen“, regt Rosche an. Als Business-Treiber bewertet der Experte den Umstand, dass die Tendenz in den Unternehmen anhalte, nicht nur einen Gateway-Server anzuschaffen, sondern die bestehenden Systeme besser auszulasten.

Gerade bei einer Firewall-Policy zeigten sich indes die derzeit existierenden Defizite. „Es hat sich ein Wirrwarr an Richtlinien gebildet, die oftmals suboptimal aufgesetzt sind“, gibt Rosche zu bedenken. Das Security-Benchmarking innerhalb von Branchen und vergleichbaren Industrien nehme deshalb weiter zu. Allein die Konvergenz von physischer und logischer Security bringe eine neue Qualität hervor, bekräftigt der Experte. Rosche hält nicht-triviale Metriken sogar bei der Verwendung von Memory-Funktionen mit Blick auf IPS-Systeme für denkbar.

Die mit Hilfe einer metrischen Analyse gefundenen Werte gilt es indes auch fortlaufend kritisch zu hinterfragen. „Ob eine Anzahl von 50 oder 100 gefundenen Computerviren pro Tag viel oder wenig ist, und welche Schlüsse sich daraus ziehen lassen, das ist so einfach nicht zu beantworten“, argumentiert Sicherheitsexperte Stefan Strobel. Das Ableiten von Metriken aus sinnvollen Kennzahlen erfordere einen soliden Regelkreislauf. Es gelte das konkrete „Überwachungsobjekt“ mit jeder einzelnen Maßnahme auf einen relevanten Soll-Ist-Vergleich abzubilden.

Absolut objektiv erhobene und messbare Daten, wie viel Zeit und Geld sich etwa beim IT-Support sparen ließen, hält Strobel indes für reine Makulatur. „Derartige meist in Selbstauskünften ermittelten Ergebnisse tun nicht weh, haben aber oftmals wenig mit der Realität zu tun“, bekräftigt der Experte. Aber auch die pauschale Aussage, Sicherheit sei ein Prozess, könne die Betriebe auf gefährliche Irrwege führen, sofern diese Behauptung nicht durch permanente Messungen an der richtigen Stelle untermauert sei.

Redakteur: Peter Schmitz

searchsecurity.de 09.01.08