Wirtschaftlichkeitsbetrachtungen von IT-Sicherheitsmaßnahmen

Maximilian Dermann
Mitglied OWASP Germany
IT-Security Architect
maximilian.dermann@hamburg.de
+49 (0) 176 48 66 3223

OWASP
Frankfurt, 25.11.08

Agenda

Das Problem

Was bedeutet Wirtschaftlichkeit?

Kosten – Einmalkosten und laufende Kosten

Nutzen – Schadenshöhe und Eintrittswahrscheinlichkeit

Allgemeine Tips und Tricks

Das Problem

- Jede Investition sollte einer Wirtschaftlichkeitsbetrachtung stand halten
- IT-Sicherheit bringt (in der Regel) keinen direkten Gewinn
- Häufig wir der Wert von IT-Sicherheit erst erkannt, wenn ein signifikanter Schaden entstanden ist
- Der Erfolg von IT-Sicherheitsmaßnahmen lässt sich nur schwer nachweisen, da Schäden in der Regel nicht budgetiert werden und somit auch nicht „eingespart" werden können

Was bedeutet Wirtschaftlichkeit?

Wikipedia:

> "Wirtschaftlichkeit ist ein allgemeines Maß für die Effizienz, bzw. für den rationalen Umgang mit knappen Ressourcen."

Berechnung (vereinfacht):

Netto-Gegenwartswert = **Nutzen – Kosten**

[Erwartungswerte, abgezinst, gemessen in Geldeinheiten]

Kosten

Bewährte Kostenbetrachtung in der IT:

Total Cost of Ownership (TCO)

setzt sich zusammen aus

- direkten Kosten (budgetierbar)
- indirekten Kosten (unproduktive Nutzung)

Kosten – *Tips und Tricks*

Bei Web-Sicherheitsmaßnahmen können die indirekten Kosten (unproduktive Nutzung) in der Regel vernachlässigt werden, wenn

- Schulungen bei den direkten Kosten berücksichtigt werden
- die eingesetzten Tools ausreichend ergonomisch sind
- die definierten Prozesse pragmatisch sind und sich in bestehende Prozesse einpassen lassen

da die Prozesse von IT-Spezialisten durchgeführt werden (sollten)

Kosten - *direkte Kosten*

direkte Kosten können

- Einmalkosten

oder

- laufende Kosten

sein

Einmalkosten

Frage: was muss ich (am besten im Rahmen eines Projekts) einmalig ausgeben für

- ☐ Hardwarebeschaffung
- ☐ Softwarebeschaffung
- ☐ Softwareentwicklung
- ☐ Projektleitung/Koordination
- ☐ Beratung
- ☐ Neudefinition bzw. Anpassung der Betriebsprozesse
- ☐ Schulungen
- ☐ …

Einmalkosten – *Tips und Tricks*

- Kosten immer ermitteln, nicht schätzen
- Nach Möglichkeit ein Angebot einholen
- Dabei die relevanten Stellen (Einkauf) mit einbeziehen
- Nach Projektpreisen fragen
- Angeben, wenn das Angebot noch unverhandelt ist
- Wenn kein Angebot eingeholt werden kann, angeben, dass es sich um Listenpreise handelt

Laufende Kosten

Frage: was muss ich regelmäßig ausgeben,
pro Komponente bzw. Prozess für

- ☐ Hardwaresupport
- ☐ Softwaresupport
- ☐ Betriebskosten (bei Outsourcing oder interner Verrechnung)
- ☐ Prozesskosten
- ☐ Rechenzentrumskosten (Miete, Strom, Kühlung, …)
- ☐ …

Laufende Kosten – *Tips und Tricks*

- Bei laufenden Kosten sind Schätzungen zulässig
- Bei Schätzungen sollten Spannen (best case, worst case) angegeben werden
- Die angegebenen Spannen sollten überschaubar sein (z.B. 35 – 45 T € und nicht 10 – 100 T €)
- Achtung: das Management wird immer die worst case Schätzung annehmen

Nutzen

Bei IT-Sicherheitsmaßnahmen ergibt sich der Nutzen aus **vermiedenem Schaden**

Schaden = Schadenshöhe x Eintrittswahrscheinlichkeit

Schadenshöhe

Die potentielle Schadenshöhe wird **pro (Web-)Anwendung** berechnet.

Schäden durch unzureichende Sicherheitsmaßnahmen können durch Verletzung von

- **Vertraulichkeit** der Daten
- **Integrität** der Daten
- **Verfügbarkeit** der Anwendung oder mit der Anwendung verbundener Drittsysteme

auftreten

Schadenshöhe – *Tips und Tricks*

- Die potentielle Schadenshöhe wurde möglicherweise schon im Rahmen des Risikomanagements, zumindest für die betroffenen Geschäftsprozesse ermittelt

Schadenshöhe - *Vertraulichkeit*

Frage: handelt es sich bei den von der Anwendung gespeicherten oder verarbeiteten Daten um

- ☐ Betriebsgeheimnisse
  - ☐ Finanzdaten **[SOX]**
  - ☐ Entwicklungsdaten
- ☐ Personaldaten **[Datenschutzgesetze]**
- ☐ Kundendaten
  - ☐ Kreditkartendaten **[PCI DSS]**
  - ☐ Zugangsdaten
  - ☐ Vertragsdaten
  - ☐ persönlichen Daten

Schadenshöhe - *Vertraulichkeit*

Monetäre Bewertung

- Imageschaden und dadurch Verlust von Kunden (Marketingabteilung fragen, wie teuer eine Imagekampagne wäre, um den Imageschaden zu beseitigen)
- potentielle Strafzahlungen (PCI, Basel II, Vertragsstrafen)
- Schadenersatzforderungen

Schadenshöhe - *Integrität*

Frage: was kann passieren, wenn Daten mutwillig verändert werden

- ☐ ohne Kenntnis der betroffenen Prozesse
- ☐ mit Kenntnis der betroffenen Prozesse

Gibt es in den betroffenen Prozessen manuelle Kontrollen, bei denen eine Veränderung der Daten auffallen würde?

Schadenshöhe - *Integrität*

Monetäre Bewertung

- Wie viel Aufwand ist für die Wiederherstellung der Daten notwendig?
- Wie lange fallen Anwendungen, die auf diese Daten zugreifen während der Wiederherstellungszeit aus (siehe Verfügbarkeit)?
- Können Waren/Dienstleistungen erschlichen werden?

Schadenshöhe - *Verfügbarkeit*

Schäden auf Grund von Verfügbarkeitseinschränkungen sollten nach Dauer bewertet werden
(z.B. 10 min, 30 min, 2 h, 6 h, 24 h, 3 d)

- ☐ Welche Geschäftsprozesse sind betroffen?
- ☐ Gibt es Notfallprozesse?
- ☐ Kann auf andere Tätigkeiten ausgewichen werden?
- ☐ Wie viele Kunden sind betroffen?

Schadenshöhe - *Verfügbarkeit*

Monetäre Bewertung:

- Berechnung interne Kosten
  (interner Stundensatz x Ausfallzeit [h])
- Berechnung Umsatzausfall
  (durschnittlicher Tagesumsatz über die betroffene Anwendung, umgerechnet auf Ausfallzeit)
- Bewertung Imageschaden
  (siehe Vertraulichkeit)

Eintrittswahrscheinlichkeit

Die Eintrittswahrscheinlichkeit ist die am schwierigsten zu schätzende Komponente.

Die Angabe einer Spanne (best case – worst case) ist deshalb sinnvoll.

- Hochrechnung anhand bisheriger Incidents auf eigenen Systemen

- statistische Auswertung/Extrapolation in der selben Branche oder bei ähnlichen Unternehmen

Eintrittswahrscheinlichkeit – *Tips und Tricks*

- Wenn keine belastbare Schätzung möglich ist, eine gefühlte Häufigkeit angeben (z.B. 1 mal in 10 Jahren) und anhand dieser die Wahrscheinlichkeit (10% p.a.!) angeben

- Zur Not die Eintrittswahrscheinlichkeit ganz weglassen und nur die (konservativ berechneten) Schadenspotentiale angeben

Allgemeine Tips und Tricks

- Sicherheit als (allgemeine) Projektanforderung definieren
- Überprüfen, ob Sicherheitsmaßnahmen Voraussetzung für (neue) Geschäftsmodelle oder Erschließung neuer Märkte sind
- Über Geschäftsprozess getriebene Compliance-Projekte (PCI, SOX, Basel II, …) prozessübergeifende Sicherheitsvorgaben machen

Allgemeine Tips und Tricks

- Idealerweise bereits bestehende Sicherheitsmaßnahmen wirtschaftlicher gestalten
- Maßnahmenpakete nach Schutzbedarf schnüren und die Anwendungen den Paketen zuordnen
- Schäden durch unzureichende Sicherheitsmaßnahmen (im Rahmen eines regulären Prozesses) sofort erfassen und mindestens Quartalsweise so hoch wie möglich ins Management melden, um ein Bewusstsein für den Wert von Sicherheitsmaßnahmen zu bilden