Risiko-Analyse für die Informationstechnologie von Hochschulen

Markus von der Heyde
info@vdh-it.de

Abstract: Hochschulen haben sich in den vergangenen Jahren in die Abhängigkeit von Verfügbarkeit, Vertraulichkeit und Integrität der durch IT gestützten Prozesse begeben. Dennoch haben nur wenige Hochschulen die Grundwerte der Sicherheit institutionsweit definiert oder die eingegangenen Risiken konkret abgeschätzt und benannt. Das eigentliche Ziel: nur sehenden Auges definierte Risiken einzugehen, wird oftmals verfehlt. Dieser Beitrag zeigt einen Weg und dessen Vorteile auf, wie auf überschaubare Weise die Unsicherheit, welche Risiken überhaupt bestehen, maßgeblich verringert werden kann. Als Ergebnis einer verfahrensspezifischen Risikoanalyse entsteht jeweils ein priorisierter Plan von Maßnahmen. Dieses Verfahren kann darüber hinaus als ein essentieller Baustein dienen, eine Zertifizierungen nach ISO 27001 zu erreichen.

1 Ausgangslage

Hochschulen haben sich in den vergangenen Jahren so wie viele Wirtschaftsunternehmen auch in die Abhängigkeit von Verfügbarkeit, Vertraulichkeit und Integrität der durch Informationstechnologie (IT) gestützten Prozesse begeben. Durch den Wandel von der dezentralen IT-Versorgung (Empfehlung der DFG bis 2005) zu den integrierten Versorgungskonzepten (DFG Empfehlung der DFG ab 2006) wurden komplexe und hoch vernetzt IT-Prozesse geschaffen. Bereits 2004 hat der ZKI als Dachverband der Rechenzentren der Hochschulen die Einführung der IT-Sicherheit als zentralen durch die Leitung gesteuerten Prozess empfohlen [Arb05]. In Hochschulen erscheint jedes formale Verfahren, IT-Sicherheit institutionell zu verankern und Risiken in derart vernetzten Systemen abzuschätzen häufig zu aufwändig. Es wurde in einer Studie gemeinsam mit einer kleinen Hochschule und einem externen Beratungsunternehmen ein Weg definiert, dennoch ein Maß für die Risiken der verschiedenen IT-Verfahren zu definieren um daraus einen priorisierten Plan von offenen Maßnahmen ableiten zu können.

2 Grundzüge der Risiko-Analyse

Aufbauend auf der klaren Abgrenzung einzelner IT-Verfahren (Begriff hier nach den Definitionen des BSI [Bun09]) wird der Schutzbedarf bzw. die maximale Schadenshöhe für Verletzungen der Verfügbarkeit, Vertraulichkeit oder der Integrität ermittelt. In einem zweiten Analyseschritt wird der Erfüllungsgrad der bereits implementierten Sicher-

erschienen im Tagungsband der INFORMATIK 2011
Lecture Notes in Informatics, Band P192
ISBN 978-3-88579-286-4
weitere Artikel online:
http://informatik2011.de/519.html

heitsmaßnahmen als eine Abschätzung für die Eintrittswahrscheinlichkeit von Ereignissen betrachtet. Über eine Transformationsmatrix wird der Erfüllungsgrad mit einem Katalog von standardisierten Bedrohungen in Beziehung gesetzt, um daraus den Mangel an bedrohungsspezifischen Schutzmaßnahmen zu ermitteln. Aus dem Maß der Wahrscheinlichkeit und der Schadenshöhe wird eine klassische Risiko-Matrix gefüllt, so dass diejenigen Bedrohungen mit der höchsten Schadenspotential und dem geringstem Schutz besondere Priorität erhalten. Letztlich kann diese Priorität wieder auf die ausgangs betrachten Maßnahmen zurückgeführt werden um für die bisher nicht realisierten Maßnahmen eine Priorität in der Bearbeitung festlegen zu können.

3 Abgrenzung der IT-Verfahren

Um eine spezifische Analyse vornehmen zu können, ist zunächst die Abgrenzung des zu betrachtenden Verfahrens vorzunehmen. Dabei wird festgehalten, aus welchen angrenzenden Verfahren Daten übernommen werden, oder welche Prozess-Schritte anderer Verfahren von dem eigentlich zu betrachtenden Verfahren abhängen. So ist zum Beispiel das eLearning abhängig von der Verfügbarkeit der Serverinfrastruktur und der Netzkommunikation; es trägt auf der anderen Seite als über Hochschulen verteile Groupware zu Finanzprojekten oder Chipkartenprojekten bei. In der folgende Analyse ist es essentiell, die Folgeschäden von angrenzenden IT-Verfahren nicht in die Bewertung des eigentlichen Verfahrens zu übertragen. Eine anschließende Analyse zur Vernetzung von IT-Verfahren wäre ansonsten unmöglich, da sich in den Grundverfahren (Netz, Stromversorgung usw.) intransparent alle Risiken ansammeln.

4 Bestimmung des Schutzbedarfs

Der erste Analyseschritt im Verfahren bewertet den Schutzbedarf eines Verfahrens bzw. zeigt die Wirkung von konkreten Vorfällen auf die Hochschule auf. Diese Analyse kann an Hand der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) definierten Schutzbedarfs-Matrix [Bun08] oder dem durch das Information Security Forum (ISF) definierten Katalog [ISF07] von Verletzungen der Grundwerte der IT-Sicherheit vorgenommen werden. In jedem Fall ist das Ergebnis dieses ersten Schrittes die Erkenntnis, welche Schadenshöhe bzw. Wirkung eine Verletzung der IT-Grundwerte maximal erreichen kann. Eine Klassifikation der Ergebnisse in z.B. drei einfach Klassen (niedrig, mittel, hoch) erleichtert den späteren Umgang mit den Ergebnissen.

erschienen im Tagungsband der INFORMATIK 2011
Lecture Notes in Informatics, Band P192
ISBN 978-3-88579-286-4
weitere Artikel online:
http://informatik2011.de/519.html

5 Einschätzung des Umsetzungsgrads übergreifend definierter Maßnahmen

In einem zweiten Schritt der Analyse werden zu allen Maßnahmen aus einem vollständigen Katalog von Maßnahmen (z.B. aus dem ISO/IEC 27001:2005 [DIN08]) geprüft, welchen Stand der Umsetzung bzw. welche Relevanz eine jede Maßnahme in Bezug zum betrachteten IT-Verfahren hat. Bereits eine dreistufige Bewertung ist im ersten Schritt als Bewertungsmaßstab ausreichend. Im Beispielprozess der Hochschule wurde die Bewertung voll erfüllt, zum Teil erfüllt oder nicht erfüllt angewendet. Wenn eine Maßnahme im Kontext des betrachteten Verfahrens keine Relevanz hat, wird die Maßnahme als nicht zutreffend klassifiziert und wirkt sich dann nicht auf den im folgenden Abschnitt definierten Erfüllungsgrad aus.

6 Zuordnung von Bedrohungen und Maßnahmen

Diese zwei Analyseschritte sind für jedes IT-Verfahren spezifisch mit dem IT-Verfahrensverantwortlichen und ggf. dem beteiligten IT Personal vorzunehmen. Die übrigen Schritte sind für alle Verfahren gleich und weitgehend automatisch umzusetzen. Dazu ist einmalig erforderlich, dass zu einem geeigneten Katalog von Bedrohungsszenarien (z.B. wieder nach einem Katalog des ISF) bewertet wird, welche Maßnahmen überhaupt geeignet sind, diesen Bedrohungen entgegen zu wirken. Somit lässt sich dann für jede Bedrohung der Erfüllungsgrad der korrespondierenden Maßnahmen errechnen. Der Erfüllungsgrad ist ein grobes Maß für die Wahrscheinlichkeit, mit welcher eine spezifische Bedrohung eintreffen könnte. Komplexere Verfahren wie z.B. das Information Risk Analysis Methologies (IRAM) vom ISF implementieren hier eine wesentlich detailliertere Vorgehensweise, um die relevanten Bedrohungen und deren Eintrittswahrscheinlichkeit abzuschätzen. In Hochschulen erscheint aber der Mehrgewinn in der Präzision den Mehraufwand vorerst nicht zu rechtfertigen.

7 Definition der Risiko-Matrix

Eine Risiko-Matrix stellt die kumulierte Wirkung von Schadenshöhe und Eintrittswahrscheinlichkeit dar. Im allgemeinen definiert man eine höhere Priorität für steigende Schadenshöhen und ebenfalls eine steigende Priorität für höhere Eintrittswahrscheinlichkeiten. Die Gewichtung der beiden Steigungen ist abhängig von der Risikofreude der Hochschule und kann in großen Teilen frei gewählt werden. In allen Fällen münden die Wahrscheinlichkeitsmaße und die Schadenshöhe in einer Risiko-Matrix, welche eine Übersicht derjenigen Bedrohungen erlaubt, welchen von der Institution mit höchster Priorität begegnet werden sollte. Häufig werden die Produkte aus einer Maßzahl für Wahrscheinlichkeit [10, 20, 30, 40] mit einer Auswirkungsstufe [5, 10, 20] multipliziert, um eine Priorität zu erhalten. Es hat sich als praktisch erwiesen, wenn diese Maßzahlen keine Vielfachen von

einander darstellen, da ansonsten die Produkte mehrdeutig sind. Eine gute Lösung ist daher die Verwendung von Primzahlen. Da die Auswirkungen sich in der Betrachtung der Grundwerte ggf. unterscheiden, werden auch die Zuordnung der Bedrohungen spezifisch für den Erhalt der Grundwerte bewertet. Die einzelnen Bedrohungen werden als Referenz am Ende in der Risiko-Matrix eingetragen.

8 Bestimmung der Priorisierung von geeigneten Maßnahmen

Die bis hierhin bestimmte Priorität kann nun direkt wieder auf die zu implementierenden Maßnahmen zurück projiziert werden. Dadurch erhält man als Ergebnis der verfahrensspezifischen Risiko-Analyse eine Priorisierung der bisher noch nicht (oder nicht ausreichend) umgesetzten Maßnahmen aus dem verwendeten Maßnahmen-Katalog. Durch die jeweiligen Vereinfachungsschritte bzw. Teilung der Ergebnisse der Analysen in drei bis fünf Kategorien ist die Risiko-Matrix einerseits übersichtlich, andererseits werden viele Aspekte auf ähnliche oder gleiche Prioritäten abgebildet. An mehreren Stellen ist es in diesem Verfahren möglich, mit kontinuierlichen Zahlen in der Bewertung zu arbeiten. In der Praxis hat sich aber gezeigt, dass die damit scheinbar erreicht Präzision keinen höheren Erkenntnisgewinn bedeutet. Erst wenn nach dem mehrfachen Durchlaufen des Verfahrens und der entsprechenden Verbesserung der Risikosituation kaum noch Differenzierungen der Bedrohungen zu erwarten wären, ist eine Überarbeitung des Maßstabs zu empfehlen.

9 Zusammenfassung

Für ein klar abgegrenztes IT-Verfahren kann die in diesem Beitrag dargestellte Risiko-Analyse folgende Ergebnisse erzielen: 1) Der Schutzbedarf bzw. die Schadenshöhe für Vorfälle in der IT für kritische Geschäftsprozesse wird erfasst. 2) Der Erfüllungsgrad von Maßnahmen, die geeignet sind, spezifischen Bedrohungen zu begegnen, wird ermittelt. 3) Wenn der Erfüllungsgrad von Schutzmaßnahmen als Maß für die Eintrittswahrscheinlichkeit von Bedrohungen aufgefasst wird, kann eine klassische Risiko-Matrix abgeleitet werden. Diese zeigt diejenigen Bedrohungen auf, welche mit einer hohen Wahrscheinlichkeit die höchsten Schäden erwirken könnten. 4) Um diesen Bedrohungen wirksam zu begegnen, kann die unter 2) vollzogene Analyse verwendet werden, um diejenigen Maßnahmen aus dem Katalog zu priorisieren, welchen einen besonderen Beitrag zur Senkung des Risikos haben könnten.

Literatur

[Arb05] Arbeitskreis für IT-Sicherheit des ZKI. IT-Sicherheit an Hochschulen. online, 2005. http://www.uni-weimar.de/cms/uploads/media/IT-Sicherheit_an_Hochschulen.pdf (Stand 29.06.2011).

[Bun08] Bundesamt für Sicherheit in der Informationstechnik (BSI). BSI-Standard 100-2. *Kapitel 4.3 der IT-Grundschutz-Vorgehensweise, Version 2.0*, 2008.

[Bun09] Bundesamt für Sicherheit in der Informationstechnik (BSI). IT-Grundschutz-Kataloge. *Glossar und Begriffsdefinitionen, 11. Ergänzungslieferung*, Seite 45 ff., 2009.

[DIN08] DIN-NIA-01-27. *Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Anforderungen (ISO/IEC 27001:2005).* Beuth Verlag, 2008.

[ISF07] ISF. The Standard of Good Practice for Information Security. online, 2007. https://www.isfsecuritystandard.com/SOGP07/index.htm (Stand 29.06.2011).

erschienen im Tagungsband der INFORMATIK 2011
Lecture Notes in Informatics, Band P192
ISBN 978-3-88579-286-4
weitere Artikel online:
http://informatik2011.de/519.html