FH Bielefeld
University of
Applied Sciences

Umfrage:
„Kosten der IT-Sicherheit“

Prof. Dr. Achim Schmidtmann, Fachbereich Wirtschaft und Gesundheit, Fachhochschule Bielefeld

Management Summary

In Rahmen der Umfrage „Kosten der IT-Sicherheit“ wurden im Zeitraum Juli bis September 2019 verschiedene Unternehmen aus Ostwestfalen-Lippe (OWL) befragt. 10 Unternehmen haben die 13 Fragen rund um das Thema IT-Sicherheit und insbesondere die Kosten der IT-Sicherheit beantwortet.

In allen Unternehmen ist IT-Sicherheit ein wichtiges Thema, wird meistens von der IT-Leitung verantwortet und ist häufig im IT-Bereich in verschiedenen (Spezial-)Stellen verankert. 60% der Unternehmen haben ein spezielles IT-Sicherheitsbudget, welches zwischen 2% und 6% des IT-Budgets ausmacht. Bis auf zwei Unternehmen kennen alle die Kosten ihrer IT-Sicherheit aber nur bei fünf Unternehmen gibt es klare Strukturen hinter diesen Kosten.

Die häufigsten Ansätze zur Ermittlung der zukünftigen Kosten sind die Expertenschätzung und der Bottom-Up Ansatz, allerdings führt nur ein Unternehmen an, dass die Qualität dieser Ansätze auch überprüft wird. Sechs Unternehmen arbeiten mit IT-Sicherheitskennzahlen, wobei die Kennzahlen „Gesamtzahl der IT-Sicherheits-Ereignisse“ und „Anzahl schwerwiegender sicherheitsrelevanter Incidents“ von der Hälfte der Unternehmen genannt wurden.

Cyber-Security-Dashboards finden bisher nur wenig Verwendung, wohingegen bereits die Hälfte der Unternehmen eine Cyber Security Versicherung abgeschlossen hat und bei zwei weiteren ist es geplant. Penetrations- und Sicherheitstests werden sogar bereits von 70% der Unternehmen durchgeführt.

Insgesamt zeigt sich, dass die Mehrheit der Teilnehmer ihre Kosten der IT-Sicherheit kennt. Die Planung der zukünftigen Kosten sowie die Qualitätssicherung der Ermittlungsverfahren wie auch der IT-Sicherheit generell offenbart aber noch einige Lücken.

Detaillierte Auswertung

Unterteilt ist die Auswertung in die Abschnitte Mitarbeiterzahl und Organisation (Fragen 1-3), IT-Sicherheitsbudget (Fragen 4-5), Kosten der IT-Sicherheit und deren Ermittlung (Fragen 6-9), Qualitätssicherung und Risikominimierung (Fragen 10-13), wobei in den jeweiligen Abschnitten jeweils die Fragen wiederholt, dann die Ergebnisse dargestellt (nur im Überblick) und kurz diskutiert werden.

Mitarbeiterzahl und Organisation

1. Wie viele Mitarbeiterinnen und Mitarbeiter hat Ihr Unternehmen?

Größte Mitarbeiterzahl	ca. 21000
Kleinste Mitarbeiterzahl	ca. 400

Durchschnittliche Mitarbeiterzahl ca. 6400

2. In wessen Verantwortung liegt in Ihrem Unternehmen die IT-Sicherheit?

Die Ergebnisse zeigen klar, dass bei allen Umfrageteilnehmern bis auf einen trotz teils unterschiedlicher Bezeichnung der Organisationseinheiten und Stellen die Verantwortung durchgängig in der IT bzw. IT-Leitung liegt. Ein Teilnehmer gibt an, dass die Gesamtverantwortung für die Informationssicherheit im Unternehmen bei der Geschäftsführung liegt. Und ein weiterer Teilnehmer hat die Geschäftsleitung zusätzlich mit angegeben. Noch eine weitere Antwort sticht etwas hervor, da hier die Verantwortung speziell im Bereich IT Operations bzw. IT Infrastruktur liegt, also in einer IT-Fachabteilung. Weitere Organisations- und Stellenbezeichnungen, die angeführt wurden und sich teilweise inhaltlich überschneiden, sind: Head of IT, Corporate IT, IT-Leitung, IT-Abteilung, CISO (Corporate Information Security Officer), IT-Sicherheitsbeauftragter und CIO.

3. Wie ist die IT-Sicherheit in Ihrem Unternehmen organisatorisch verankert?

Bemerkenswert ist, dass es in vier Unternehmen kein explizites IT-Sicherheitspersonal gibt. In diesen Unternehmen sind es z.B. Systemadministratoren, Netzwerkplaner, Systemarchitekten, die auch das Thema IT-Sicherheit mit abdecken. In den anderen Unternehmen gibt es IT-Sicherheitspersonal mit recht unterschiedlichen Bezeichnungen. Fast alle diese Stellen sind in der IT, bei einem Unternehmen finden sich Information Security Manager auch in Gruppenunternehmen.

IT-Sicherheitsbudget

4. Haben Sie ein IT-Sicherheitsbudget?

Nur in 40% der teilnehmenden Unternehmen gibt es kein spezifisches IT-Sicherheitsbudget. Alle vier Unternehmen betonen aber, dass IT-Sicherheitsinvestitionen ins IT-Budget einfließen. Ein Unternehmen hebt hervor, dass es keine eigene Kostenstelle für die IT-Sicherheit gibt.

5. Wie viel Prozent Ihres IT-Budgets macht es aus?

Der Durchschnitt der benannten Werte für das IT-Budget liegt bei 2,5%. Allerdings muss hervorgehoben werden, dass es zu einigen Prozentwerten noch Zusatzangaben gab. So hat ein Unternehmen in seinem Prozentwert keine Hardware und ein anderes keine Kosten für IT Sicherheit in der Produktion berücksichtigt. Ein weiteres Unternehmen merkt an, dass sich der Wert aus Workshop/Schulungen (Awareness) und IT-Security Appliances zusammensetzt. Außerdem gibt es den Hinweis: „wesentliche Kosten für IT Security fallen im Betrieb an“.

Setzt man diese Zahlen in Bezug zu den Umfrageergebnissen des SANS™ Institute aus dem Jahre 2016[1], wo 169 Teilnehmer mit Budgetverantwortung oder Einblick in diese befragt wurden (72% der Befragten sind in den Vereinigten Statten ansässig), so zeigt sich doch eine recht große Diskrepanz zu den dort ermittelten Budgetwerten, die zwischen 6% und 9% liegen. Ein möglicher Grund für die große Abweichung könnte darin begründet liegen, dass die Teilnehmer dieser Umfrage einige Kostenpositionen der IT-Sicherheit nicht im Budget mit einplanen.

[1] IT Security Spending Trends ©2016 SANS™ Institute

Kosten der IT-Sicherheit und deren Ermittlung

5. Kennen Sie Ihre Kosten der IT-Sicherheit?

Die Ergebnisse dieser Frage stimmen erst einmal positiv, da nur ein Unternehmen eindeutig mit „Nein“ hat und ein weiteres mit „nicht im Detail“ geantwortet hat. Dabei wurde „nicht im Detail“ ergänzt mit: „die Kosten für explizite Maßnahmen sind allerdings transparent“.

Alle Unternehmen, die mit Ja geantwortet haben, haben allerdings noch weitere Einschränkungen gemacht, da sie nur bestimmte Kosten kennen bzw. betrachten.

7. Welche Struktur verwenden Sie, um die Kosten der IT-Sicherheit weiter herunter zu brechen?

Fünf Teilnehmer der Umfrage haben mit „nein“ oder „keine“ bzw. „keine besonderen“ geantwortet. Sie arbeiten teilweise mit Standardkostenarten oder merken an, dass sie Dienstleister nutzen, deren Angebote Kostenstrukturen enthalten.

Bei den anderen fünf Teilnehmern basiert die Struktur auf dem eingesetzten Produkt bzw. Sicherheitsbereich, der Kostenstelle IT-Sicherheit oder der Unternehmensstruktur. Bei einem Unternehmen werden die Kosten der IT Sicherheit nur über allgemeine Umlageschlüssel auf Kostenstellen verteilt.

Eine Möglichkeit die Kosten der IT-Sicherheit weiter zu strukturieren wären z.B. die IT-Grundschutz-Bausteine des BSI oder der Anhang A der ISO/IEC 27001:2015.

8. Welchen Ansatz haben Sie gewählt, um die potentiellen Kosten der IT-Sicherheit zu ermitteln?

Am häufigsten und zwar vier Mal wurde die Expertenschätzung benannt. Dabei wird es sich sehr wahrscheinlich um interne und externe Experten handeln. Eine Antwort wurde auch noch um die Stichworte „Standards“ und „Ausrichtung an ISO27001“ ergänzt. Demnach wird dort auch das in Standards manifestierte Expertenwissen als Grundlage verwendet.

Zwei Unternehmen gehen Bottom-Up vor, um die Kosten der IT-Sicherheit zu schätzen. Ein Teilnehmer hat geantwortet, dass anhand der aktuellen Kosten die zukünftigen geschätzt werden, dabei handelt es sich also um eine Analogiemethode auf Basis von einem gewissen Erfahrungswissen. Bei einem Unternehmen ist der Ansatz nicht bekannt und zwei verwenden keinen bzw. „keinen speziellen“ Ansatz.

9. Wie sichern Sie die Qualität Ihres Ansatzes?

Die Antworten auf diese Frage wurden in den meisten Fällen nicht auf den Ansatz der Ermittlung der Kosten der IT-Sicherheit (siehe Frage 8), sondern generell auf die IT-Sicherheit bezogen. Nur ein Teilnehmer hat geantwortet, dass eine Plausibilitätsprüfung der Budgetanträge durch das Controlling stattfindet.

Die Frage zielte eigentlich darauf hin, ob der gewählte Ansatz, wie z.B. Expertenwissen oder Bottom-Up, und seine Ergebnisse auch regelmäßig überprüft werden im Sinne eines PDCA-Ansatzes. Stattdessen haben die Teilnehmer verschiedene Qualitätsmaßnahmen wie z.B. die Implementierung eines ISMS oder die Durchführung von Audis benannt.

Qualitätssicherung und Risikominimierung

10. Mit welchen IT-Sicherheitskennzahlen arbeiten Sie?

Sechs der zehn Teilnehmer zählen IT-Sicherheitskennzahlen auf, mit denen sie heute bereits arbeiten. Drei Unternehmen verwenden heute noch keine und bei einem Unternehmen ist die Verwendung von IT-Sicherheitskennzahlen im Aufbau. Am häufigsten benannt wurden:

- Gesamtzahl der IT-Sicherheits-Ereignisse
- Anzahl schwerwiegender sicherheitsrelevanter Incidents
- Anzahl der Security-bedingten Service-Ausfallzeiten
- Anzahl implementierter Präventiv-Maßnahmen

11. Arbeiten Sie mit Cyber-Security-Dashboards?

Cyber-Security-Dashboards sind bisher nur bei drei der zehn Unternehmen im Einsatz, wobei es sich in einem Fall nicht um ein spezielles Cyber-Security- sondern ein ITSM Dashboard handelt. Ein Dashboard ist ein Herstellercockpit und über das dritte gibt es keine weiteren Informationen.

Bei zwei Unternehmen ist das Thema in Planung bzw. im Aufbau und fünf Teilnehmer haben mit „Nein“ geantwortet. Somit scheint dieses Hilfsmittel bisher bei vielen Unternehmen eher nicht im Fokus zu sein.

12. Haben Sie eine Cyber Security Versicherung?

Wie die Abbildung 6 zeigt, haben bereits fünf der Umfrageteilnehmer eine Cyber Security Versicherung und bei zwei Unternehmen ist sie in Planung oder Diskussion. Nur drei Unternehmen geben an, dass sie noch keine derartige Versicherung haben.

Da Cyber Security Versicherungen aber ganz unterschiedliche Themen abdecken können, würde hier erst eine weitergehende Frage Aufschluss über die genaue Risikoverlagerung durch diese Versicherungen geben.

13. Führen Sie zyklische Penetrations-/ Sicherheitstests durch?

Penetrations- und Sicherheitstests sind dagegen noch etwas weiter verbreitet und werden von sieben der zehn Unternehmen regelmäßig und von einem achten unregelmäßig durchgeführt. Nur zwei Unternehmen antworteten, dass sie keine durchführen.

Auch hier würde es sicherlich noch Sinn machen, tiefer in die Details dieser Tests einzusteigen, um ihre Sinnhaftigkeit und ihren Umfang genauer zu ermitteln.

Fazit

Die Auswertung der Umfrage ermöglicht eine Bestandsaufnahme über die teilnehmenden IT-anwendenden Unternehmen. Die Beantwortung ist auch aufgrund der Verschiedenartigkeit der Unternehmen nicht repräsentativ, die Ergebnisse können aber in jedem Fall als Anregung und in Teilen auch als Benchmark dienen.

Außerdem hat die Beantwortung bei den Teilnehmern einerseits sicherlich für ein gewisses Nach- und Überdenken von IT-Sicherheitsthematiken geführt und andererseits verdeutlichen die Ergebnisse die Varianz der Ausprägungen in Detailtiefe und –breite und können damit zum Wissenstransfer beitragen.

Betont werden muss, dass die Ergebnisse der Umfrage keine direkte Verbindung zwischen der Größe der Unternehmen und der Umsetzungsquote der verschiedenen IT-Sicherheitsthemen zeigten. Die Umsetzungsquote wurde in diesem Fall über die Anzahl der Fragen, die mit „nein“ oder „keine“ bzw. mit „in Diskussion“ oder „in Planung“ im Gegensatz zu denen, die mit „ja“ beantwortet wurden ermittelt.

Den Abschluss und die Quintessenz dieser Umfrage stellen folgende vier Forderungen an ein sinnvolles IT-Sicherheitsbudget dar:

- Gießkannenprinzip muss Vergangenheit sein!
- Budgetplanung sollte auf Basis der Ergebnisse des Risikomanagements durchgeführt werden!
- Die Planung eines eigenen Sicherheitsbudgets muss losgelöst vom IT-Budget erfolgen und alle Sicherheitsaspekte umfassen!
- Nutzen Sie Frameworks und Standards als Hilfestellung!

Bielefeld im November 2019

Professor Dr. Achim Schmidtmann
Fachhochschule Bielefeld
Fachbereich Wirtschaft und Gesundheit
Interaktion 1
33619 Bielefeld
Telefon +49.521.106-5065
Telefax +49.521.106-5086
achim.schmidtmann@fh-bielefeld.de
www.fh-bielefeld.de