31

BPX.

Andreas Wisler
Fredy Schwyter

Was Manager wissen müssen!

Informations-sicherheit für KMU

Sicherheitskonzepte & praktische Umsetzung

2. Auflage

- **Gesetze & Verantwortung**
- **Grundschutz für KMU**
- **Praxis der Informationssicherheit**
- **Kosten-Nutzen-Aspekte**
- **Technologie-Grundlagen**
- **Sicherheitskonzepte umsetzen**
- **Outsourcing & Managed Security Services**
- **Praxisbeispiele**
- **Checklisten**
- **Trends**

www.bpx.ch

BPX.

Andreas Wisler
Fredy Schwyter

Was Manager wissen müssen!

Informations-sicherheit für KMU

Sicherheitskonzepte & praktische Umsetzung

2., überarbeitete Auflage

BPX-Edition
Rheinfelden/Schweiz

BPX Best Practice Xperts
E-Mail edition@bpx.ch
Internet www.bpx.ch

Andreas Wisler, Fredy Schwyter

Informationssicherheit für KMU
Sicherheitskonzepte & praktische Umsetzung

Vorwort von Prof. Dr. Bernhard Hämmerli

Rheinfelden/Schweiz, BPX-Edition 2013
ISBN 978-3-905413-24-3

Hinweis: In diesem Booklet wird bei Bezeichnungen die männliche Form verwendet. Dies dient lediglich der Lesefreundlichkeit und schliesst die weibliche Form mit ein.

Herstellung: BPX-Edition, Rheinfelden/Schweiz

Druck und Verarbeitung: Druckerei galledia ag, Flawil

1 Vorwort

Das Geheimnis hinter effektiver Informationssicherheit heisst: Sie muss gelebt werden! Diese Aussage aus dem Awareness-Film von Sun Microsystems wurde im vorliegenden Booklet von den zwei Autoren speziell für KMU treffend umgesetzt.

Informationssicherheit beginnt beim Management. Da besteht aus meiner Erfahrung gesehen noch viel Nachholbedarf. Es scheint mir wichtig, dass die Geschäftsführung sich mit diesem Thema zuerst ausführlich befasst, die richtigen Massnahmen plant und anschliessend Kontrollprozesse zur Prüfung einsetzt. Es ist wie bei einem Hausbau: Der Besitzer muss Vorgaben machen und danach die Ausführung kontrollieren. Damit lässt sich viel Ärger vermeiden.

Die Erfahrung zeigt, wie Katastrophen-Vorsorge das Überleben sichert. Auch KMU sind heutzutage vom funktionierenden Informationsfluss zunehmend abhängig. Viele Beispiele belegen: Wer bei einer Katastrophe einen durchdachten Vorsorgeplan umsetzen kann, hat gute Chancen zu überleben. Wer diese Möglichkeit nicht hat, meldet Konkurs an.

Den beiden Autoren ist es bestens gelungen, den sinnvollen Einsatz von Standards aufzuzeigen. Nicht jeder muss das Rad neu erfinden. Es sind die wichtigsten Standards beschrieben: fürs Management ISO/IEC 27001, für die Technik die Grundschutztools vom deutschen Bundesamt für Sicherheit in der Informatik und für exportorientierte Firmen mit Lieferung in die USA die Common Criteria.

Für die interessierten Leser findet sich auch eine gute Ausführung über die State-of-the-Art Technology im Sicherheitsbereich. Diese ist für KMU vor allem wertvoll, um Ausfallkosten bei der IT zu sparen.

Viele praktische Hinweise helfen dabei, Informationssicherheit zu realisieren und zu leben. Solche Sicherheit ist nicht nur auf IT beschränkt: Auch Betriebsprozesse von Information, Gesetze und Mitarbeitende sind von höchster Wichtigkeit für das Unternehmen. Lesen Sie dazu ins Booklet hinein!

Prof. Dr. Bernhard Hämmerli

Hochschule Luzern

2 Management Summary

Informationssicherheit steht heute zuoberst auf der Prioritätenliste weitsichtiger KMU-Führungskräfte. In allen Betrieben spielt Information eine entscheidende Rolle, und diese gilt es zu schützen. Oder haben Sie schon einen General gesehen, welcher seine Soldaten schutzlos in den Krieg schickt?

Der Vergleich mit Krieg ist insofern zulässig, als jeder Computer am Internet von überall in der Welt her angegriffen werden kann. Und die Angriffsszenarien werden immer ausgefeilter. Dazu kommt, dass nur ausgebildetes Personal die wichtigen Informationen sicher handhaben kann. Von nicht ausgebildetem Personal richtige Entscheidungen zu erwarten, ist sinnlos. Vier wichtige Punkte möchten wir besonders hervorheben:

- Informationssicherheit (IS) ist eine Managementaufgabe
- Ein Katastrophen-Vorsorgeplan hilft, im Worst Case zu überleben
- Für IS und deren Unterhalt muss Budget bereitgestellt werden
- Zuverlässiges Personal gibt es nur mit Ausbildung

Kleinere KMU haben meist die personellen Ressourcen nicht, um einen eigenen Information Security Officer einzustellen. In diesen Fällen ist es sinnvoll, diese Aufgaben an ein spezialisiertes Unternehmen auszulagern. Doch auch beim Outsourcing von IS bleibt die Verantwortung dafür bei der Unternehmensführung.

Gelebte IS bringt auch eine Reihe von Vorteilen, z.B.:

- Das Vertrauen der Kunden steigt
- Kredite werden günstiger
- Mit Vorausdenken lässt sich viel Geld sparen
- Weniger Ärger wegen nicht zuzuordnender Fehler
- Es gibt weniger Kundenklagen
- Gut ausgebildetes Personal unterstützt Sie
- Ihr Unternehmen ist für den Notfall vorbereitet und kann überleben

In diesem Booklet erfahren Sie:

- Worauf zu achten ist bei der Entwicklung von Informationssicherheit
- Wie die Gesetzeslage aussieht
- Welche Standards Ihnen helfen
- Wo die heutigen Gefahren liegen
- Wie Sie Risiken in den Griff bekommen können
- Welche Technologien Ihnen zur Verfügung stehen
- Wie Sie IS nach State-of-the-Art umsetzen können

«Die Anforderungen an und die Abhängigkeit von der IT nehmen immer mehr zu. Auch die Komplexität hat stark zugenommen, viele Projekte stehen zudem unter grossem Zeitdruck. Auf der anderen Seite nehmen die Gefahren und Risiken ebenfalls rapide zu. Das organisierte Verbrechen hat längstens den Weg ins Internet gefunden und verdient viel Geld mit Angriffen, Erpressungen, mit Spam und Malware. Daher ist es essenziell wichtig, auf die neuen Bedrohungen vorbereitet zu sein und entsprechende Massnahmen proaktiv zu ergreifen. Dieses Booklet soll Ihnen einen Überblick bieten.»

Andreas Wisler

Das Geheimnis von guter Informationssicherheit liegt darin, dass sie gelebt wird!

«Auch mittelständische Unternehmen werden zunehmend von IT-Sicherheitsvorfällen bedroht – Beispiele sind der Verlust von geistigem Eigentum oder die Nichtverfügbarkeit der angebotenen Kerndienstleistungen. Im Gegensatz zu Grossfirmen sind kleine und mittelständische Unternehmen jedoch oft nicht in der Lage, den entsprechenden Aufwand zum Schutz der Informatikmittel und der darauf basierenden Abläufe zu leisten – eine mögliche Lösung kann hier in der Nutzung seriöser ‹Managed Security Services› liegen.»

Prof. Dr. Hannes Lubich
FHNW

3 Managementverantwortung

Die Geschäftsleitung hat die Verpflichtung, Massnahmen zur Gewährleistung von Informationssicherheit im Unternehmen umzusetzen. Folgende gesetzliche Bestimmungen enthalten Forderungen dazu:

- Buchführungsvorschriften: Buchführungsrecht, Revisionsgesetz (neue Version 2007) mit Kontrolle des internen Kontrollsystems inklusive Risikobeurteilung.
- Aufbewahrungspflicht: Normalerweise 10 Jahre. Diese Zeitspanne kann zwecks Beweispflicht aber auch länger sein.
- Öffentlich-rechtliche Vorschriften, z.B. bezüglich Auskunftspflicht, Berufsgeheimnisse usw.
- Strafrecht, z.B.: Unbefugtes Eindringen in ein Datenverarbeitungssystem oder Datenbeschädigung kann nur geahndet werden bei Nachweis von speziellen Schutzmassnahmen.
- Aktienrecht: definiert die Organhaftung von Verwaltungsrat und Geschäftsleitung. Sie kann neu bis zur Haftung mit dem persönlichen Eigentum gehen.
- Vertragsrecht: Gewährleistung der angebotenen Leistungen, Schadenersatz.
- Branchenspezifische Rechtsvorschriften: beispielsweise in der Pharmabranche, bei Banken, Versicherungen, im Gesundheitswesen oder in der Nahrungsmittelverarbeitung.
- Datenschutzgesetz: Gesetz über den Schutz von Personendaten auf kantonaler und eidgenössischer Ebene.
- Persönlichkeitsrecht: Überwachung, Genugtuung, Schadenersatz.

Aufgrund dieser Aufzählung könnte manch einer auf die Idee kommen, gesetzliche Vorschriften seien der Hauptgrund zum Einsatz von Sicherheitsmassnahmen. Tatsache ist jedoch, dass Gesetze meist erst dann erlassen werden, wenn deren Einhaltung bereits gängige Praxis ist – oder zur Vermeidung von grösserem Schaden.

Die Durchsetzung von Compliance mit bestehenden Gesetzen liegt in der Verantwortung des Verwaltungsrats und der Geschäftsleitung. Der Einsatz heutiger Informations-Sicherheits-Management-Systeme erleichtert und unterstützt diese Aufgabe wesentlich.

3.1 Managed Security Services

Vergibt ein Unternehmen Teile seiner Informationsverarbeitung an ein externes Unternehmen in Form von Outsourcing, dann müssen zusätzliche Kriterien beachtet werden. Wichtige Punkte dabei sind:

- Die Verantwortung bleibt beim Auftraggeber
- Überprüfbare Service Level Agreements (SLA)
- Gemeinsames Sicherheitskonzept
- Einhaltung der Lizenzbedingungen
- Umsetzung branchenspezifischer Vorschriften
- Datenschutzgesetze, v.a. bei grenzüberschreitenden Transaktionen

Um die wichtigste Ressource in heutigen Unternehmen zu sichern, ist es unabdingbar, dass das oberste Management sich diese Aufgabe zuoberst auf die Prioritätenliste setzt. Mitarbeitende richten sich automatisch auf die Vorgaben der Geschäftsleitung aus. Fehlen diese Vorgaben oder haben sie eine niedere Priorität, dann kann nicht von Informationssicherheit gesprochen werden.

Beispiel: Bekommt eine Sekretärin von ihrem Chef den Auftrag, mit seinem Passwort die Verträge kurz auszudrucken, zu denen sie mit ihrem Passwort keinen Zugriff hat, dann zeugt dies zwar von grossem Vertrauen seitens des Chefs, aber diese Sekretärin wird alle anderen Sicherheitsvorschriften nur als lästiges Übel empfinden. Sie wird vermutlich versuchen, wo immer es geht, diese zu umgehen. (Z.B.: Anstatt die Verträge der Geschäftspartnerin verschlüsselt zuzustellen, werden diese unverschlüsselt übertragen.) Und was für die Chefsekretärin gut ist, wird von allen anderen Mitarbeitenden in Kürze nachgeahmt. Damit verlieren Aufwendungen für die Informationssicherheit an Wert.

Oft ist es noch schlimmer, da man sich der Gewissheit hingibt, «wir tun ja etwas für die Informationssicherheit», z.B. durch regelmässige Backups. Da diese aber mangels Kapazität nie durch Restore (zurückspielen und auf Funktionstüchtigkeit testen) überprüft wurden und oft auch nicht in feuersicheren Behältern ausserhalb des Betriebes lagern, werden sie im Falle einer Feuersbrunst oder bei Wasserschaden im Serverraum nicht mehr zu gebrauchen sein.

Dazu kommt, dass gerade grössere Schäden dort vorkommen, wo das Personal denkt: Das kann bei uns nie passieren.