

# Augen auf!

**Kaum ein IT-Verantwortlicher eines kleinen oder mittelgrossen Unternehmens in der Schweiz kann sich heute vorstellen, ohne Firewall eine Verbindung ins Internet herzustellen. Wer keinen aktuellen Virenschutz auf seinen Servern und PCs installiert hat, gilt bestenfalls als Optimist. Und wer ohne tauglichen Backup ein geschäftskritisches System betreibt – lassen wir das.**

VON ROLF BRUNNER

## Was ich nicht weiss...

Die drei wesentlichen Massnahmen der IT-Security (Firewall, Virenschutz, Backup) sind in den meisten KMU realisiert und decken die populärsten IT-Risiken ab. Was also soll mit einem IT-Security Assessment denn noch erreicht werden? Was bringt es, wenn ein IT-Security-Spezialist mit tausend Fragen irgendwelche Schwachstellen herauszufinden versucht?

### Assessment:

- ▶ Abschätzung
- ▶ Bemessung
- ▶ Beurteilung
- ▶ Bewertung
- ▶ Einschätzung

## ...macht mich nicht heiss

«IT-Security generiert – so wie sämtliche Anstrengungen im Bereich der Sicherheit – vor allem Kosten und wenig Nutzen. Sicherheit beeinträchtigt oftmals die Funktionalität und Flexibilität eines Systems. Die IT hat primär zu funktionieren und soll nicht zum Selbstzweck werden.»

So oder ähnlich wird häufig argumentiert, wenn es darum geht, in die IT-Security des eigenen Unternehmens zu investieren. Oft fehlt das Bewusstsein, inwiefern die Geschäftsprozesse von den dazu erforderlichen Daten, Applikationen, Systemen, Netzwerkverbindungen und der physischen Infrastruktur abhängig sind. Diese Abhängigkeit ist für eine KMU ebenso relevant wie für eine grosse Unternehmung. Oder der Umgang mit gesetzlichen Vorgaben im Bereich Datenschutz, Straf- oder Vertragsrecht kann am ehesten mit dem Begriff «heisse Kartoffel» zum Ausdruck gebracht werden. Zudem verspricht die Werbung, dass mit dem Einsatz dieses oder jenes Produktes



### Rolf Brunner

ist Informatik-Projektleiter mit eidg. FA und Absolvent des Nachdiplomstudiums Informatik-Sicherheit an der HSW Luzern. Er ist als Consultant im Bereich IT-Security bei der Firma isec ag in Luzern tätig.



die Sicherheit des Unternehmens gewährleistet sei. Wie viel Sicherheit braucht eine KMU denn sonst noch?

## Dennoch...

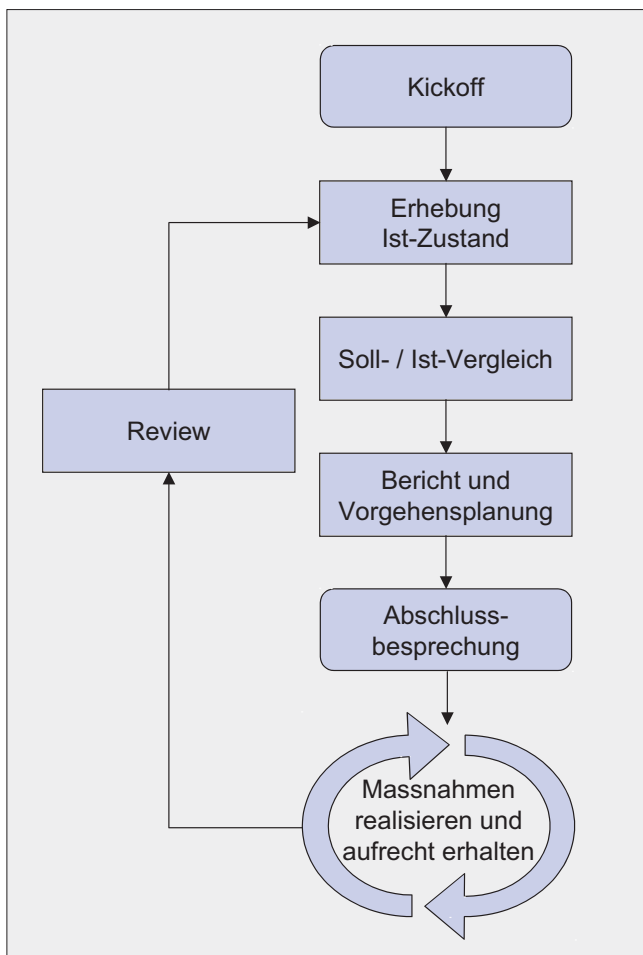
Wozu also ein IT-Security Assessment? Unternehmen, welche ein solches Assessment durchführen, zeichnen sich durch eine oder mehrere der folgenden Eigenschaften aus:

- ▶ Es besteht der Wille der Geschäftsleitung, sich selber in einem wesentlichen Bereich den Spiegel vorzuhalten.
- ▶ Die Sorgfalt gegenüber Kunden, Mitarbeitenden und Geschäftspartnern wird ernst genommen.
- ▶ Qualität drückt sich eher als Teil der Unternehmenskultur aus als in entsprechenden Zertifikaten (wobei das eine das andere nicht ausschliesst).
- ▶ Ein «Schlüsselerlebnis» hat das Bewusstsein geschärft.
- ▶ IT-Security wird integral, im Zusammenhang mit anderen Sicherheitsthemen betrachtet.

## ...Augen auf!

Wie läuft denn nun ein IT-Security Assessment ab, und welche Themenbereiche werden betrachtet? Um mit geringem Aufwand ei-

nen möglichst grossen Nutzen zu erzielen, ist ein vereinfachtes Vorgehen gemäss IT-Grundschutz sinnvoll. Dies setzt keine aufwändige Risikoanalyse voraus und hilft, auf direktem Wege geeignete Sicherheitsmassnahmen zu identifizieren. Stützt man sich dabei auf ein Hilfsmittel, welches einen «Best Practice»-Ansatz



verfolgt, so fördert dies die Akzeptanz der aus dem Assessment hervorgehenden Massnahmenempfehlungen.

Wesentlich ist zudem, dass IT-Security integral betrachtet wird. An vielen Punkten bestehen Synergien mit einem allenfalls vorhandenen Qualitätsmanagement-System. Zudem ist IT-Security kein rein technisches Thema, sondern umfasst in gleichem Masse auch die Bereiche Organisation und Recht. Der Ablauf eines IT-Security Assessment gliedert sich in mehrere Phasen, welche in den folgenden Abschnitten kurz erläutert werden.

### **Kickoff**

In einem ersten Gespräch mit derjenigen Person eines Unternehmens, welche für die IT-Security verantwortlich zeichnet, werden die Ziele, Rahmenbedingungen, Abgrenzungen und Schwerpunkte des Assessment definiert. Ausgehend von einem Netzwerkübersichtsplan wird die Abhängigkeitsmatrix erstellt und eine Klassifikation der Applikationen nach Vertraulichkeit, Verfügbarkeit und Integrität vorgenommen.

### **Erhebung des Ist-Zustandes**

Auf der Basis von Checklisten, wie diese beispielsweise das «Sicherheitshandbuch für die Praxis» bietet, wird der Ist-Zustand erhoben. Dazu werden Interviews mit verschiedenen Personen geführt. Beispielsweise mit dem IT-Verantwortlichen für die technischen Aspekte, dem Personalleiter bei Fragen rund um das Thema Weisungen, Richtlinien und Arbeitsverträge oder einem Mitarbeitenden, um dessen Wahrnehmung der IT-Security zu erfassen. Die Aussagen aus den Interviews werden punktuell nachgeprüft. Ergänzend dazu werden technische Schwachstellenanalysen innerhalb des Netzwerks der Unternehmung sowie aus dem Internet durchgeführt (Penetrationstests). Hierzu gehört in der Regel eine Überprüfung der Passwortqualität. Auch die Sichtung vorhandener Dokumente oder eine Begehung der IT-Räume gehören zum Repertoire eines IT-Security Assessment.

### **Soll-Ist-Vergleich**

Die gewonnenen Erkenntnisse werden den Massnahmenempfehlungen gegenübergestellt und auf deren Erfüllungsgrad geprüft. Wichtig ist, dass Branche, Abhängigkeiten und Prioritäten der Unternehmung berücksichtigt werden. Diese Unterscheidung ist zentral, denn eine soziale Institution beispielsweise hat völlig andere Anforderungen im Bereich der Vertraulichkeit als ein Maschinenbau-Unternehmen. Die Messung von Erfüllungsgraden enthält immer ein gewisses Mass an Subjektivität. Aus diesem Grund ist es vorteilhaft, wenn eine externe, kompetente Person diese Beurteilung vornimmt. Dadurch wird die eigene Betriebsblindheit umgangen, und es steht genügend Erfahrung im Hintergrund, damit

aus dem Assessment ein vergleichbares und ausgewogenes Resultat hervorgeht.

Basierend auf dem Soll-Ist-Vergleich wird der Handlungsbedarf in Form von Massnahmenempfehlungen abgeleitet. Auch hier werden die Rahmenbedingungen und Bedürfnisse der Unternehmung berücksichtigt, um das richtige Mass an Sicherheit zu finden.

### **Bericht und Abschlussbesprechung**

Die gewonnenen Erkenntnisse werden als Bericht dokumentiert. Dieses Dokument gibt den Verantwortungsträgern der Unternehmung Aufschluss über die festgestellten Stärken, Schwächen und den Handlungsbedarf. Doch dies ist eigentlich erst der Anfang der Geschichte, denn die Sicherheit wächst erst, wenn die erste Massnahme auch tatsächlich umgesetzt wird. Es ist deshalb von zentraler Bedeutung, dass die Massnahmenempfehlungen klar, einfach realisierbar, mit Prioritäten versehen und einer verantwortlichen Person zugeordnet sind. Dies erlaubt ein Vorgehen in kleinen, «verdaubaren» Schritten.

### **Wie weiter?**

Ein IT-Security Assessment allein verschafft noch kein Mehr an Sicherheit. Aber es bringt die Erkenntnis, wo man heute steht. Dies wiederum ist eine Voraussetzung, um sich Ziele zu setzen und den Weg zum Ziel zu bestimmen. Dem Unternehmen soll deshalb ein gangbarer Weg aufgezeigt werden, wie das gewünschte Mass an Sicherheit zu erreichen ist. Dieser Weg besteht in der Regel aus den folgenden Elementen:

#### ► Sofortmassnahmen

Sie decken die wesentlichsten Schwachstellen ab, sind innerhalb von zwei bis drei Wochen realisierbar, erzeugen keine oder nur minimale Kosten und können mit den eigenen personellen Ressourcen realisiert werden.

#### ► Auftragsliste

Die Auftragsliste umfasst alle weiteren Massnahmen, welche planbar sind und je nach Priorität kurz- bis mittelfristig angegangen werden sollten.

#### ► Kontrolle und Aufrechterhaltung

IT-Security ist kein Projekt, sondern ein Prozess. Die Trennung von Umsetzung und Kontrolle der IT-Security ist sinnvoll. Demzufolge gehört auch ein Kontrollinstrument, beispielsweise in Form einer Checkliste für das Management, zum Umfang eines IT-Security Assessment.

Der Fortschritt in der IT-Security soll nach einiger Zeit verifiziert werden. Zudem verändert sich die IT-Infrastruktur und auch die Risikosituation jeder Unternehmung laufend. Es macht daher Sinn, in regelmässigen Abständen, z.B. alle 12 bis 24 Monate, ein Review durchzuführen.

### **Was also bringt's?**

Der Nutzen eines IT-Security Assessment für eine KMU ist:

- Schwachstellen und mögliche Risiken werden transparent.
- Eine umfassende und mit geringem Aufwand verbundene Standortbestimmung.
- Investitionen in die IT-Security erfolgen gezielt und werden planbar.
- Ein praxisorientiertes Vorgehen mit klaren Ergebnissen.

## **Sicherheitshandbuch für die Praxis**



#### **Umfang**

A4-Ordner mit ca. 300 Seiten, CD-ROM

#### **Verlag**

Verlag Gisler, Altdorf, ISBN-Nr. 3-9521208-3-9

#### **Preis**

CHF 248.- (inkl. MwSt., exkl. Versandkosten)

#### **Bezugsquelle**

isec ag, 6002 Luzern ([www.isec.ch](http://www.isec.ch))

Das «Sicherheitshandbuch für die Praxis» richtet sich explizit an kleine bis mittlere Unternehmen und Verwaltungen. Es zeigt mögliche Bedrohungen und Gefahren auf, gibt praktische Hinweise und unterbreitet Lösungsvorschläge. Die auf der dazugehörigen CD-ROM enthaltenen Checklisten und Musterdokumente erleichtern zudem die Umsetzung der vorgeschlagenen Sicherheitsmassnahmen und ebnen den Weg zu angemessener Informations- und IT-Sicherheit.