

Das IT-Sicherheitskonzept

Garant für eine gesunde Informatik

Von Pascal Schoch

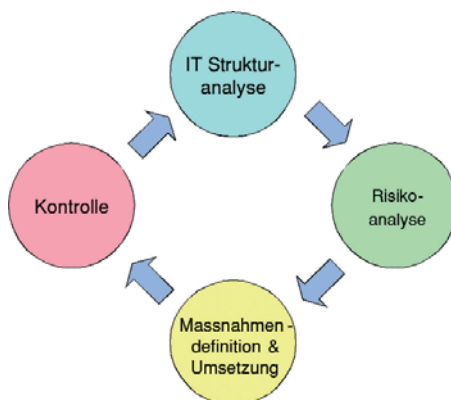
Viele Unternehmen vernachlässigen bewusst oder unbewusst die Sicherheit ihrer Informatik. Zu oft begnügen sie sich mit dem Erwerb einer Firewall und betrachten damit das Thema als erledigt. In der Praxis zeigen sich leider zudem weitere Sicherheitsdefizite.

So sind Security-Verantwortlichkeiten häufig nicht konsequent festgelegt, es ist kein vergleichbares Sicherheitsniveau in den Abteilungen vorhanden oder es fehlt ein schriftlich fixiertes Datenschutzkonzept. Damit setzen sie sich einer existenziellen Gefahr aus. Dies gilt umso mehr für Unternehmen, welche mit sensitiven Patienten- oder Kundendaten arbeiten.

Sicherheit ist das Produkt eines permanenten Sicherheitsmanagements

Hohe Sicherheit ist das Produkt eines permanenten Sicherheitsmanagements und wird nicht mit der blossen Installation einer Firewall erreicht. Dabei ist das Ziel, die Daten vor Verlust der Vertraulichkeit, Verlust der Integrität und Verlust der Verfügbarkeit zu schützen. Für die Erlangung dieses Zieles bietet es sich an, ein Sicherheitskonzept zu erstellen. Ein solches Konzept beschreibt neben vorhandenen und benö-

tigten Komponenten (z.B. Firewalls, Antiviren-Software, aber auch physische Elemente wie Zutrittsmechanismen, Überwachungskameras) auch die angetroffenen Risiken, notwendigen Massnahmen und Prozesse (z.B. Einschränkung der Benutzerrechte, Passwort-Policy, Datenarchivierung), welche für die Realisierung und Aufrechterhaltung des angestrebten Sicherheitsniveaus notwendig sind.



Das Sicherheitskonzept als permanenter Prozess

In vier Schritten zum eigenen IT-Sicherheitskonzept

Viele Unternehmen stufen es als unnötig ein, extra ein IT-Sicherheitskonzept zu erstellen. Leider ist mit der wachsenden digitalen Vernetzung der Unternehmung, vor allem durch das Internet, die Angriffsfläche für Hacker und Datendiebstahl bzw. -missbrauch geradezu explosionsartig gewachsen. Für einen flächendeckenden Schutz ist es darum unumgänglich, die gesamte Unternehmung nach möglichen Sicherheitschwachstellen zu durchleuchten und entsprechende Massnahmen schriftlich im Sicherheitskonzept zu definieren.

In einem ersten Arbeitsschritt wird darum zuallererst die «IT-Strukturanalyse» erstellt. Mit dieser Analyse wird der Ist-Zustand festgehalten (in der Regel durch eine Inventarisierung der gesamten IT) und so die aktuelle Lage vor Ort ermittelt. Zu beachten ist, dass die Strukturanalyse keine Wertung enthält sondern sich auf die Beschreibung der Ist-Situation beschränkt.

Das Sicherheitskonzept als permanenter Prozess

Schwachstelle	Gefahr	Schutzbedarf	Sicherheitsmassnahmen
Backup-Datenträger sind nicht einheitlich gekennzeichnet.	Irrtümliche Überschreibung von Datenträgern.	Verfügbarkeit; niedrig	Beschriftungskonzept erstellen.
Hohe Temperatur im Rechnerraum.	Systemausfall wegen Überhitzung.	Verfügbarkeit; mittel	Klimaanlage einbauen.
Benutzerpasswörter werden nicht periodisch geändert.	Missbrauch von Passwörtern wird erleichtert.	Vertraulichkeit, Integrität; mittel	Passwörter alle 30 Tage ändern.
Uneingeschränkter Zutritt zu schutzbedürftigen Räumen.	Zutritt durch Unberechtigte.	Vertraulichkeit; hoch	Zutrittskonzept inklusive Einschränkungen einführen.
Keine Virenüberprüfung vorhanden.	Datenverlust und Systemausfall durch Virusinfektion.	Verfügbarkeit; hoch	Antiviren-Software installieren.
Betriebssystem wird nicht aktualisiert.	Hackerangriff via Security-Lecks im Betriebssystem.	Vertraulichkeit, Integrität; hoch	Patch-/Update-Management einführen.

Beispiel einer Risikoanalyse

Am Ende dieses Arbeitsschrittes sollte ein Dokument vorliegen, welches als Inventurkatalog aufzeigt, wo welche IT-Mittel (Hard- und Software) eingesetzt sind.

In einem nächsten Schritt wird die ange-troffene Situation auf Sicherheitsmängel und Bedrohungen untersucht. Das Ziel einer solchen Risikoanalyse ist es zu ermitteln, mit welchem Aufwand Anwendungen, Systeme, Kommunikationsverbindungen und Räume vor Beeinträchtigungen der Vertraulichkeit, Integrität und Verfügbarkeit geschützt werden können. Dieser Sicherungsbedarf orientiert sich am möglichen Schaden, der bei einer effektiven Beeinträchtigung entstehen würde. Da der mögliche Schaden manchmal nicht genau quantifizierbar ist, bietet sich in der Praxis bei der Risikoanalyse eine Kategorisierung durch Einstufung wie z.B. «niedrig», «mittel» und «hoch» an. Die Erstellung einer Risikoanalyse kann sehr zeitaufwändig sein. Sie ist aber ein wichtiger Bestandteil des Sicherheitskonzeptes. Je genauer die Risikoanaly-

se ist, desto nützlicher und vor allem effektiver ist auch das Sicherheitskonzept. Es ist darum ratsam, die notwendige Zeit für eine saubere Erstellung einzuplanen.

Nachdem die Informationen aus der Sicherheits- und Risikoanalyse vorliegen, geht es darum, die notwendigen Massnahmen zur Behebung der erkannten Schwachstellen zu definieren und umzusetzen. Die Reihenfolge bzw. Priorisierung der Massnahmen sollte aufgrund des festgehaltenen Schutzbedarfes vorgenommen werden. Ratsam ist, für jede einzelne Massnahme eine verantwortliche Person zu bestimmen, inklusive Zeitplan für die Umsetzung sowie Abnahmekontrolle.

Nur ein aktuelles Sicherheitskonzept garantiert eine gesunde Informatik

Wie zu Beginn erwähnt, ist Sicherheit ein Prozess und nicht eine einmalige Tätigkeit. Auch das IT-Sicherheitskonzept ist darum als

wiederkehrende Tätigkeit zu betrachten. Mit den sich ändernden Bedrohungen ändert sich gleichzeitig der Schutzbedarf der Unternehmung, und damit muss auch das IT-Sicherheitskonzept erneuert werden. Nur ein aktuelles Sicherheitskonzept kann als Garant für eine gesunde Informatik dienen.

Zum Autor: Pascal Schoch war nach seinem Betriebswirtschaftsstudium als Product Manager im Bereich Electronic Commerce Solutions bei Swisscom tätig. Seit August 2000 ist er als Product Manager bei Aspectra AG für den Bereich Application Outsourcing verantwortlich.

Weitere Informationen:

Aspectra AG

Stationsstrasse 17

8003 Zürich

Telefon 044 296 56 56

Telefax 044 296 56 57

E-Mail info@aspectra.com

Internet www.aspectra.com