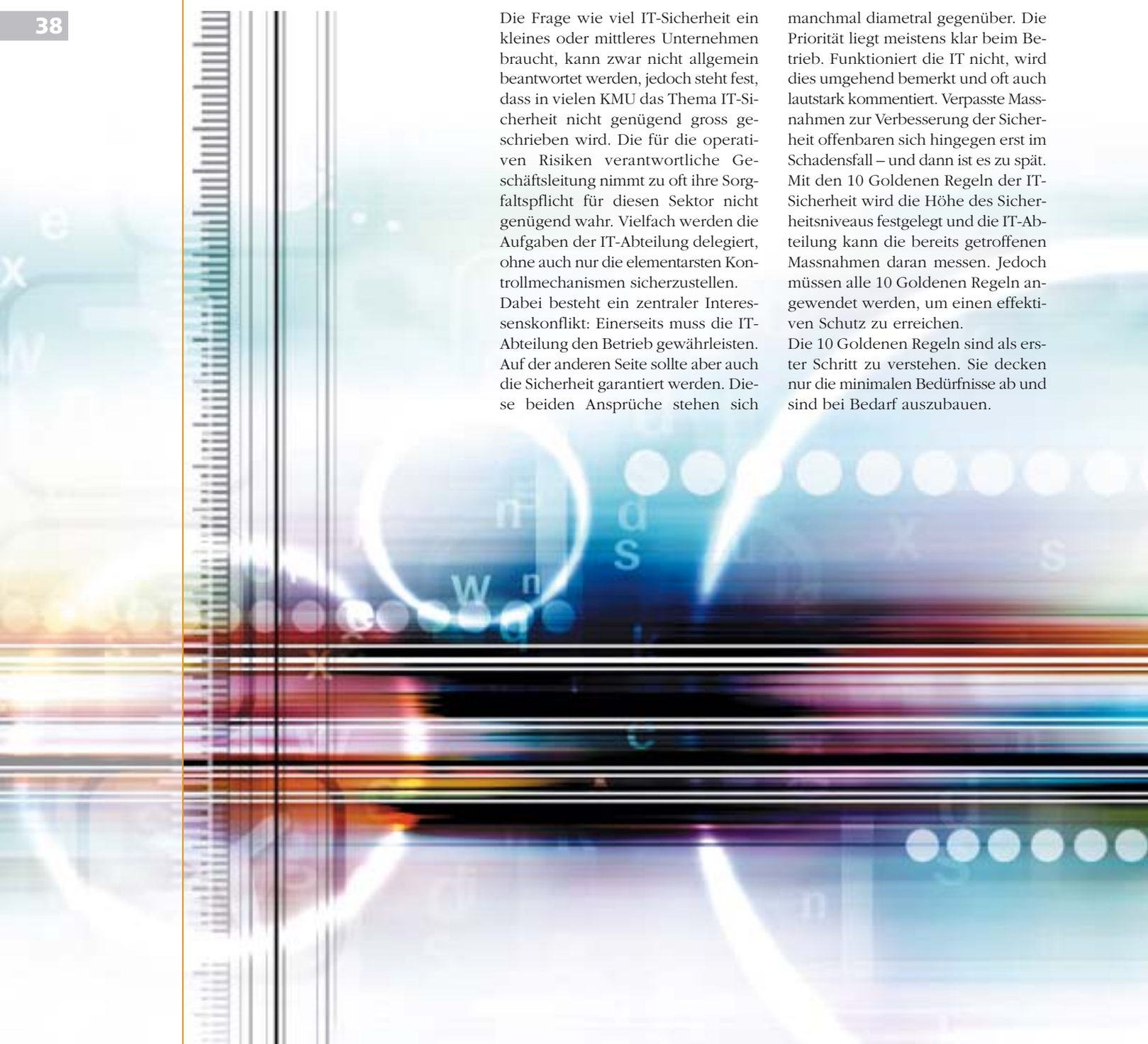
Wie viel IT-Sicherheit brauchen Unternehmen?

Mit den 10 Goldenen Regeln der IT-Sicherheit wird das Ziel eines minimalen Schutzes verfolgt, der in allen kleinen und mittleren Unternehmen (KMU) umgesetzt werden sollte.

Der Autor ist Leiter des Competence Center IT-Security an der Hochschule für Wirtschaft Luzern sowie Leiter der Arbeitsgruppe KMU der Stiftung InfoSurance Schweiz.

von Carlos Rieder



Die Frage wie viel IT-Sicherheit ein kleines oder mittleres Unternehmen braucht, kann zwar nicht allgemein beantwortet werden, jedoch steht fest, dass in vielen KMU das Thema IT-Sicherheit nicht genügend gross geschrieben wird. Die für die operativen Risiken verantwortliche Geschäftsleitung nimmt zu oft ihre Sorgfaltspflicht für diesen Sektor nicht genügend wahr. Vielfach werden die Aufgaben der IT-Abteilung delegiert, ohne auch nur die elementarsten Kontrollmechanismen sicherzustellen.

Dabei besteht ein zentraler Interessenskonflikt: Einerseits muss die IT-Abteilung den Betrieb gewährleisten. Auf der anderen Seite sollte aber auch die Sicherheit garantiert werden. Diese beiden Ansprüche stehen sich manchmal diametral gegenüber. Die Priorität liegt meistens klar beim Betrieb. Funktioniert die IT nicht, wird dies umgehend bemerkt und oft auch lautstark kommentiert. Verpasste Massnahmen zur Verbesserung der Sicherheit offenbaren sich hingegen erst im Schadensfall – und dann ist es zu spät.

Mit den 10 Goldenen Regeln der IT-Sicherheit wird die Höhe des Sicherheitsniveaus festgelegt und die IT-Abteilung kann die bereits getroffenen Massnahmen daran messen. Jedoch müssen alle 10 Goldenen Regeln angewendet werden, um einen effektiven Schutz zu erreichen.

Die 10 Goldenen Regeln sind als erster Schritt zu verstehen. Sie decken nur die minimalen Bedürfnisse ab und sind bei Bedarf auszubauen.

Die 10 Goldenen Regeln – IT-Sicherheit zweckmässig umgesetzt

Die Arbeitsgruppe KMU der Stiftung InfoSurance hat diese Regeln zusammengestellt und publiziert unter www.infosurance.ch/de/kmu.htm. Mit der Idee «besser 10 Regeln umgesetzt als 100 geplant» wurde ein pragmatischer Ansatz gewählt. Die Autoren sind sich bewusst, dass mit diesem Vorgehen nicht alle Risiken abgedeckt werden, sicher jedoch die wichtigsten.

Regel Nr. 1 – Verantwortlichkeiten definieren

Wer ist für was verantwortlich? Zum Beispiel für die Datensicherung oder den Update der Virensoftware? Missverständnisse können unnötige und zum Teil gravierende Störfälle zur Folge haben. Dies ist sehr einfach zu verhindern, wenn die verantwortlichen Personen klar definiert sind.

Regel Nr. 2 – Datensicherung

Die tägliche Datensicherung ist heute in den meisten Unternehmen eine Selbstverständlichkeit. Werden einzelne Sicherungsbänder extern aufbewahrt? Wird mit Generationen gearbeitet (Tages-, Wochen-, Monats-Bänder)? Wann wurde das Wiedereinlesen der Daten ab Band das letzte Mal getestet? Werden wirklich alle Daten gesichert? Diese Fragen müssen geklärt sein, um die Effektivität der Datensicherung zu garantieren.

Regel Nr. 3 – Schutz vor Computerviren

Noch nie wurden so viele neue Computerviren und -würmer in die Welt gesetzt wie in den letzten Monaten.

10 GOLDENE REGELN DER INFORMATIONSSICHERHEIT

1. Verantwortlichkeiten definieren
2. Datensicherung
3. Schutz vor Computerviren
4. Sichere Verbindung ins Internet
5. Software aktuell halten
6. Umgang mit Passwörtern
7. Zutrittsregelung
8. Benutzerrichtlinien
9. Sensibilisierung
10. Ordnung und Informationsschutz

Nur ein aktivierter und topaktueller Virenschutz kann vor dieser Gefahr schützen. Deshalb müssen die neuen Virensignaturen auf allen Servern und Clients inklusive Notebooks regelmässig aktualisiert werden.

Regel Nr. 4 – Sichere Verbindung ins Internet

Alle Verbindungen nach aussen sind potenzielle Sicherheitsrisiken, über die unberechtigte Dritte ins Netzwerk eindringen können. Der Einsatz einer korrekt konfigurierten Firewall ist zwingend nötig. Zusätzlich muss die Firewall auch regelmässig gewartet und in ihrer Funktion überprüft werden. Beim Einsatz von Wireless LAN sind die möglichen Sicherungsmassnahmen unbedingt zu aktivieren.

Regel Nr. 5 – Software aktuell halten

Regelmässig wird über neu entdeckte Schwachstellen informiert. Die Hersteller verbessern ihre Programme und stellen Patches und Hotfixes zur Verfügung. Diese müssen aber nun auch auf allen Servern und Clients im Unternehmen installiert werden. Die meisten Schäden aus den letzten grossen Angriffen hätten durch die rechtzeitige Einspielung der entsprechenden Reparaturprogramme verhindert werden können.

Regel Nr. 6 – Umgang mit Passwörtern

Bekanntlich ist der unsorgfältige Umgang mit Passwörtern die häufigste Sicherheitsverletzung in einem Unternehmen. Ein sicheres Passwort muss mindestens acht Zeichen lang sein und neben Zahlen und Buchstaben (gross und klein) auch Sonderzeichen enthalten.

Regel Nr. 7 – Zutrittsregelung

Was nützt das beste Passwort, wenn Unberechtigte ohne Mühe Zutritt zum Serverraum oder zur Datensicherung erhalten? Jedoch müssen nicht nur die Server und Sicherungskopien geschützt werden. Vertrauliche Informationen sind im ganzen Unternehmen zu finden, weshalb der Zutritt klar geregelt sein muss.

Regel Nr. 8 – Benutzerrichtlinien

Für alle Geräte bestehen Betriebsvorschriften. Für den Umgang mit Informatikmitteln werden jedoch selten Benutzerrichtlinien erlassen und noch seltener eingehalten. Das Verhalten der Benutzer muss mit kommunizierten Richtlinien geregelt werden. Zu einfach können installierte Sicherheitsbarrieren durch bewusstes oder unbewusstes Verhalten der Benutzer umgangen werden.

Regel Nr. 9 – Sensibilisierung

Der sicherheitsbewusste Umgang mit Informationen und Informatik muss ein Teil der Unternehmenskultur sein. Deshalb müssen die Mitarbeitenden entsprechend sensibilisiert werden. Durch Wachsamkeit und mit gesundem Menschenverstand können viele der plumpen Angriffe auf die Informatik abgewehrt werden.

Regel Nr. 10 – Ordnung und Informationsschutz

Vertrauliche Dokumente gehören verschlossen. Deshalb sind die Arbeitsplätze entsprechend ordentlich zu verlassen. Die neuen Möglichkeiten mit der Informatik verlangen nach einem strukturierten Ablagesystem, einheitlich über das ganze Unternehmen. Damit können regelmässige Suchaktionen nach erstellten Dokumenten verhindert werden. Hier steckt noch sehr viel Optimierungspotenzial.

Wie anpacken?

Schrittweise

Oft wird vor lauter Bäumen der Wald nicht mehr gesehen. Erfahrungsgemäss gibt es am Anfang einiges zu tun. Mit kleinen Schritten können die Aufgaben erfüllt werden. Zur Einführung empfiehlt es sich zum Beispiel, monatlich eine der 10 Goldenen Regeln umzusetzen. Der Umfang ist überschaubar und innerhalb eines Jahres wird das angestrebte Niveau auf diese Weise erreicht.

Stetig

Die Umsetzung der IT-Sicherheit ist ein Prozess, der dauernd weiterentwickelt werden muss. Immer wieder müssen die getroffenen Massnahmen überdacht und an die neuen Bedürfnisse angepasst werden.

Konsequent

Die 10 Goldenen Regeln müssen konsequent umgesetzt werden. Bewusst wurde nur ein minimales Set von Regeln definiert, dafür sind diese vollumfänglich zu realisieren.

Gleichmässig

Das zu erreichende Sicherheitsniveau muss ausgewogen und gleichmässig sein. Was hilft eine hochsichere Firewall, wenn vertrauliche Informationen in den Büros offen herumliegen (Passwort auf Post-it-Zettel an den Monitor geheftet) und somit frei zugänglich sind?

Es tun!

Die Informationen sind vorhanden und so aufbereitet, dass eine einfache Umsetzung möglich ist. Die Voraussetzungen sind somit gegeben. Packen wir es an!

Eine detaillierte Beschreibung der 10 Goldenen Regeln ist zu finden unter www.infosurance.ch.

Im «Sicherheitshandbuch für die Praxis» finden sich vertiefte Hinweise mit Vorlagen und Checklisten (www.sihb.ch). ◆

INTERVIEW MIT PAUL HASEN, MITGLIED DER GESCHÄFTSLEITUNG, BW DIGITRONIK AG

McAfee stellt mit IntruShield eine neue Produkt-Familie für die Netzwerksicherheit vor. Diese ermöglicht eine Echtzeit-Erkennung von Angriffen auf Firmen- und Behördennetzwerke und soll auch die komplexesten Netzwerke vor DoS-Attacken schützen. Drei Fragen an Paul Hasen, Mitglied der Geschäftsleitung von bw digitronik ag und Anbieter von E-Security-Lösungen:

kommunikation: *Welche Vorteile bietet das neue IDS-System von McAfee?*

Paul Hasen: Bei IntruShield handelt es sich um ein echtes Intrusion Prevention System (IPS), das in der Lage ist, Angriffe nicht nur zu erkennen, sondern die unerwünschten Datenpakete direkt zu blockieren. Dadurch wird die Sicherheit wesentlich erhöht – blosses Erkennen genügt heute nicht mehr – und der Analyseaufwand drastisch reduziert, weil das System die Entscheidungen selbst trifft.

Für welche Firmen eignet sich die IntruShield-Lösung?

IntruShield eignet sich am besten für Firmen und Organisationen, für die ein Datenverlust oder ein Systemausfall einen hohen Verlust bedeutet. Dies trifft für die meisten grösseren Firmen aber z. B. auch für Shop-Betreiber zu.

Wie werden sich Firmen in Zukunft vor Netzwerkattacken schützen müssen?

Der Einsatz einer Firewall und eines Virenschutzes am Gateway gehören heute zur Standard-Sicherheitsausrüstung jeder Firma. Um die heutigen Angriffe abwehren zu können, genügt dies aber nicht mehr. Es werden zusätzliche Schutzfunktionen benötigt. Intrusion Prevention ist der nächste Schritt. Die gegenwärtige Nachfrage am Markt bestätigt dies.