EINE THEMENZEITUNG VON MEDIAPLANET

Nr. 1/September 2013

MEDIA PLANET

ICT SOLUTIONS

5 TIPPS FÜR DIE RICHTIGE BYOD-STRATEGIE

CSIRT
IT-Sicherheitszertifikat erstmals in der Schweiz

CLOUD-ARTEN
Welches sind die Unterschiede

VERSCHLÜSSELUNG
Wie werden Daten für Angreifer unlesbar

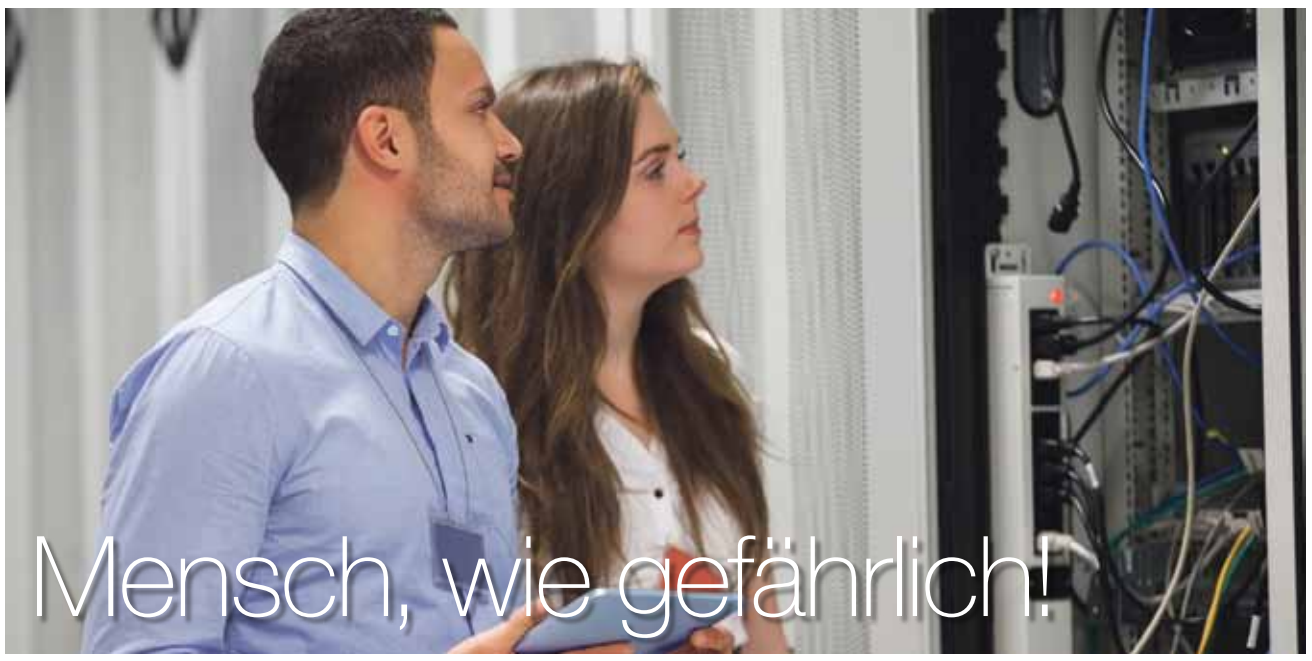
SENSIBLE DATEN
Die Bedeutung des Sicherheitsmanagements

SICHERE WOLKEN

So lässt Sie **Ihre Cloud** nicht im Regen stehen.

FOTO: CORBIS

INSPIRATION



Mensch, wie gefährlich!

■ **Frage:** Wie schützen Sie Ihr Unternehmen vor Bedrohungen der Informationssicherheit?
■ **Antwort:** Die grösste Gefahr lauert intern. Darum: Sensibilisieren Sie Ihre Mitarbeiter.

Aktuelle Fälle wie beim Schweizer Nachrichtendienst oder die NSA-Spionage zeigen auf, dass die realen Bedrohungen heute durch die eigenen Mitarbeitenden, untaugliches oder ganz fehlendes Risikomanagement, fehlende Mittel und Ressourcen für die Planung und Umsetzung der Sicherheitsmassnahmen, fehlende oder unzureichende Weisungen, mobile Endgeräte Cloud-Computing, soziale Netzwerke, falsche Zugriffsberechtigungen und unsichere Software-Applikationen stark zugenommen haben.

Sicher immer wichtiger

Die dynamischen Veränderungen in Wirtschaft, Gesellschaft und Technik schaffen neue Gefahren und Risiken, die sich kombiniert mit anderen begleitenden Ereignissen wie Wirtschaftsspionage zu einem oft stark unterschätzten Risiko entwickeln können.

So überrascht es nicht, dass der Informationssicherheit eine immer grössere Bedeutung auf wirtschaftlicher, gesellschaftlicher, politischer und rechtlicher Ebene zukommt.

«Die Herausforderung besteht folglich darin, Ihre Daten und Ihr Knowhow mit angemessenen technischen und organisatorischen Sicherheitsmassnahmen auf Basis einer zuverlässigen und möglichst vollständigen Risiko-Analyse zu schützen», erklärt Wolfgang Sidler, Inhaber der Sidler Information Security GmbH, «und ein ausgewogenes Gleichgewicht zwischen den Risiken, der Benutzerfreundlichkeit und den Kosten herzustellen.»

Gefährlicher Mitarbeiter

Zusätzlich erhöhen sich die Risiken durch Geschäftstätigkeiten im Ausland, und nehmen schneller zu, als wir dies möchten, sind komplexer und von grösserer Tragweite. Die grössten Gefahren sind fahrlässiger Datenverlust oder Datendiebstahl durch das eigene Fehlverhalten oder durch die eigenen Mitarbeitenden. Natürlich gilt es aus Sicht der Unternehmensleitung, hohe Strategieziele wie Flexibilität, Effizienz und Innovation umzusetzen. Gleichzeitig müssen aber auch die Kosten gesenkt, die Produktivität gesteigert und die Wettbewerbsfähigkeit verbessert werden. Und genau diese Unternehmensziele können dank einer angemessenen Sicherheitsstrategie mit weniger Risiken und höherer Agilität umgesetzt werden. Es ist wichtig zu verstehen, dass der Sicherheitsgedanke als IT-Grundsatz gut im Unternehmen verankert sein muss.

Laut Sidler sollten sich Verwaltungsräte folgende Fragen stellen:
1. Kennen Sie die Risiken und Schwachstellen Ihrer IT-Infrastruktur?
2. Welchen Schaden kann eine Sicherheitslücke Ihrer Unternehmensreputation und Markenwahrnehmung zufügen?
3. Sind Ihre Mitarbeitenden genügend geschult und sensibilisiert in Bezug auf den Umgang mit Daten und dem Internet?
4. Sind Ihre Sicherheitsweisungen vollständig, aktuell und verständlich?
5. Verfügen Sie über ein aktives Risikomanagement und ein Notfallkonzept?

Teure Firewall reicht nicht

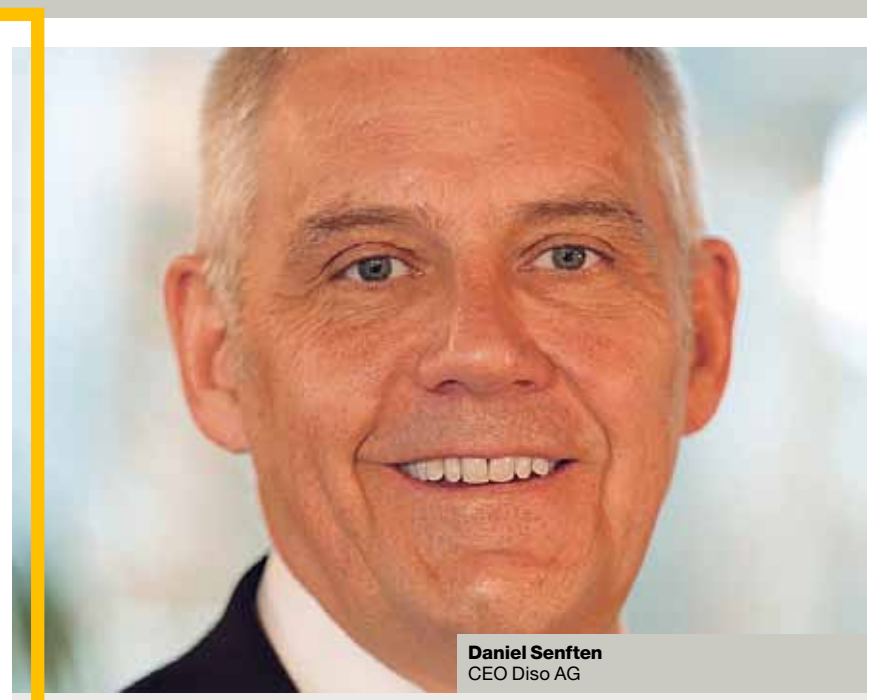
Es lohnt sich, Zeit und Geld zu investieren, um Mitarbeitende für Sicherheitsrisiken zu sensibilisieren und klare Richtlinien aufzustellen. Denn die teuersten Firewalls und Security-Lösungen bringen Ihnen nichts, wenn Ihre Mitarbeitenden durch ein falsches Verhalten die Hintertüren für Cyber-Angriffe, etwa durch die Verwendung der Dropbox etc. öffnen. Ziel ist, dass die Restrisiken bekannt sind und durch die verantwortlichen Stellen akzeptiert und getragen werden.

SUSANNE MEIER
redaktion.ch@mediaplanet.com

TIPPS

ZUR SICHERHEIT

■ Besser fünf umgesetzte Sicherheitsmassnahmen als 20 geplante.
■ Reduzieren Sie die Komplexität Ihrer IT-Infrastruktur.
■ Eine Sicherheitsmassnahme darf nicht mehr kosten als das eigentliche Risiko.
■ Konzentrieren Sie sich darauf, nicht selbst die Lösungen umzusetzen, sondern managen Sie aktiv die externen Provider.
■ Stetige Sensibilisierung auf allen Stufen.



Daniel Senften
CEO Diso AG

Selber mitbringen – auch bei der Technik

„Bring Your Own Device» (BYOD) ist in Begriff, der die Nutzung eigener Geräte in der Geschäfts- und Bildungslandschaft beschreibt. Diese Entwicklung ist zwar praktisch und günstig für die Unternehmen, doch sie birgt auch Risiken.

«Ein grosser Vorteil von BYOD ist, dass die Endgeräte der Mitarbeiter dank höherer Rechen- und Speicherleistung häufig besser ausgestattet sind als die unternehmenseigenen PCs», erklärt Daniel Senften, CEO der DISO AG. Doch in jedem Fall müssen firmenpolitische Grundsätze berücksichtigt werden. Firmen mit sehr engem Kundenkontakt (Banken, Versicherungen) haben oft strengere Richtlinien als reine Dienstleistungsunternehmen.

Firmeninterne Daten können missbraucht werden

Die grösste Gefahr beim Einsatz von BYOD besteht darin, dass der Zugriff auf firmeninterne Daten missbraucht werden kann: Entweder durch Mitarbeiter, die sich nicht an Richtlinien halten, oder durch den Verlust des mobilen Geräts. «Hier bieten jedoch bereits heute einige Hersteller die Möglichkeit des Löschens von Daten aus der Ferne an», sagt Daniel Senften.

Wenn sich ein Unternehmen überlegt, ob BYOD in Frage kommt, ist es am wichtigsten, zuerst die sicherheitsrelevanten Punkte zu klären. Daniel Senften: «Es empfiehlt sich, die Richtlinien im Umgang mit Datenschutz und Sicherheit entsprechend zu ergänzen; ausserdem sollte das Vorgehen beim Austritt des Mitarbeiters schriftlich geregelt werden.» Eine weitere Schwierigkeit ist, dass private Geräte nicht mehr durch die firmeneigene IT überwacht werden können, was die Installation und den Betrieb unterschiedlichster Software erschwert.

Mitarbeiter gehen vorsichtiger mit eigenen Geräten um

Doch trotz der Risiken hat sich gezeigt, dass Mitarbeiter mit eigenen Endgeräten wesentlich vorsichtiger und sorgfältiger umgehen als mit entsprechenden Geräten einer Unternehmung. Es gilt also: Können die sicherheitsrelevanten Themen entsprechend gelöst werden, gibt es keinen Grund, BYOD in Firmen nicht zu fördern. Daniel Senften fügt an: «In unserer Firma setzen etwa 20 Prozent der Belegschaft eigene Geräte ein. Bis jetzt haben wir damit sehr gute Erfahrungen gemacht.»

KATHRIN FINK
redaktion.ch@mediaplanet.com