Datenschutz im Kreuzfeuer

Pannen wie beim Schweizer Nachrichtendienst (NDB) oder die NSA-Spionage zeigen auf, dass Bedrohungen durch die eigenen Mitarbeitenden, mangelhaftes Risikomanagement, fehlende Mittel für die Planung und Umsetzung der Sicherheitsmassnahmen, BYOD, Cloud-Computing, soziale Netzwerke, falsche Zugriffsberechtigungen und unsichere Software-Applikationen stark zugenommen haben.

Von Wolfgang Sidler

Die rasanten Veränderungen in Wirtschaft, Gesellschaft und Technik schaffen neue Gefahren und Risiken, welche sich kombiniert mit anderen begleitenden Ereignissen wie etwa 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.

Angemessen und ausgewogen

Die Herausforderung besteht folglich darin, kritische Daten und Know-how mit angemessenen technischen und organisatorischen Sicherheitsmassnahmen auf Basis einer zuverlässigen und möglichst vollständigen Risiko-Analyse zu schützen und ein ausgewogenes Gleichgewicht zwischen den Risiken, der Benutzerfreundlichkeit und den Kosten herzustellen.

Zusätzlich werden die Risiken mit Geschäftstätigkeiten im Ausland erhöht und nehmen schneller zu, als wir dies wahrnehmen möchten. Sie sind zudem 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, die hohen 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 mit einer angemessenen Sicherheitsstrategie mit weniger Risiken und höherer Agilität umgesetzt werden. Es ist hierbei wichtig, zu verstehen, dass das Sicherheitsfundament als IT-Grundschutz solide im Unternehmen verankert sein muss.

Fragen, die Verwaltungsräte und GL-Mitglieder sich stellen sollten:

- Kennen wir die Risiken und Schwachstellen unserer IT-Infrastruktur?
- Welchen Schaden kann eine Sicherheitslücke für die Unternehmensreputation und Markenwahrnehmung bedeuten?
- Sind unsere Mitarbeitenden genügend geschult und sensibilisiert in Bezug auf den Umgang mit Daten und dem Internet?
- Sind unsere Sicherheitsweisungen vollständig, aktuell und verständlich?
- Verfügen wir über ein aktives Risikomanagement und ein Notfallkonzept?

Public Cloud

Als Benutzer einer Public-Cloud-Lösung (z.B. Dropbox, Amazon, Office 365 von Microsoft, Google etc.) weiss man nicht, auf welchen Systemen, in welchem Rechenzentrum und in welchem Land der Provider die Daten speichert. Bereits seit Juni 2011 ist bekannt, dass die US-Behörden selbst auf europäische Cloud-Daten zugreifen dürfen. In den entsprechenden Service Level Agreements (SLA) kann zum Beispiel der folgende Passus stehen: «Unter bestimmten Umständen kann der Provider Daten ohne Ihre vorherige Zustimmung weitergeben.»

Cloud-Computing ist in diesem Zusammenhang also nicht ungefährlich. Wer jedoch einen Schweizer Cloud-Provider nutzt, kann davon ausgehen, dass seine Daten in der Schweiz gespeichert werden. Zusätzlich bietet ein solcher Cloud-Provider eine sehr hohe Verfügbarkeit und Sicherheit für die kritischen Daten; so sind sie wahrscheinlich besser geschützt als jetzt im Unternehmen selbst. Der Schweizer Cloud-Provider garantiert eine sehr hohe Verfügbarkeit, erstellt täglich eine Datensicherung und garantiert vertraglich, dass die schützenswerten Daten mit den bestmöglichen technischen und organisatorischen Sicherheitsmassnahmen vor dem Zugriff durch Dritte sicher sind.

Wie kann man sich schützen?

In Anbetracht der weltweit verschärften Konkurrenzsituation und einer steigenden Abhängigkeit von modernen Informations- und Kommunikationssystemen wird es immer wichtiger, sich gegen illegale Nutzung des eigenen Wissens zu schützen. Mit zunehmender Vernetzung kommt der Sicherheit der IT-Infrastruktur höchste Priorität zu. Folgende präventiven Massnahmen können unter anderem ergriffen werden:

- **Personensicherheit:** Vor jeder Neuanstellung – speziell für sensible Bereiche – empfiehlt es sich, die Identität und Referenzen des Bewerbers zu überprüfen. Diesen Punkt sollte man auch bei Hilfskräften (z.B. Reinigungspersonal) nicht aus den Augen lassen.
- **Verschlüsselung:** Firmen-Know-how sollte strikte durch eine geeignete Verschlüsselung der Festplatten und USB-Sticks geschützt werden. Wer vertrauliche Dokumente via E-Mail versendet, verschlüsselt die E-Mail und deren Inhalt. Nur mit einer angemessenen Verschlüsselung kann die Vertraulichkeit gewahrt bleiben.
- **Passwörter:** Starke Passwörter sind zu verwenden und diese niemals an Dritte weiterzugeben. Es darf keine Passwortliste unverschlüsselt gespeichert oder ausgedruckt werden.
- **USB-Sticks:** USB-Sticks unbekannter Herkunft gehören an keinen Rechner oder Notebook. Anschluss verboten! Man sollte selbst einem vertraute USB-Sticks und CDs vorab auf Viren prüfen, bevor man diese verwendet. Im gleichen Atemzug schliesst man keinen eigenen Stick an einen unbekannten PC oder ein Notebook an, denn die Daten auf dem USB-Stick können schnell, unbemerkt und ohne Spuren zu hinterlassen auf den PC kopiert werden.
- **Handy und PDA:** Eine Code-Sperre ist das absolute Minimum.

Doch da sind noch viele Punkte mehr. Dinge, an die man meist nicht gleich als Erstes denkt. In der Öffentlichkeit etwa sollte man keine vertraulichen Gespräche während einer Bahn- oder Flugreise oder selbst im Restaurant führen. Man könnte ausgehorcht werden.

Vertrauliche Unterlagen gehören im Büro weggeschlossen; der Arbeitsplatz sollte jeweils aufgeräumt (Clear Desk) verlassen werden und keine Datenträger (CDs) und Dokumente mit sensiblem Inhalt ungeschreddert in den Papierkorb wandern. Wer seinen Arbeitsplatz auch nur für kurze Zeit verlässt, der aktiviere doch rasch den Bildschirmschoner. Weitere Punkte:

- **E-Mail:** Vertrauliche E-Mails sollten nur verschlüsselt versendet werden – nach einer nochmaligen Überprüfung der Empfänger vor dem Senden! Das Senden von Word-Dokumenten (DOC) in einer E-Mail ist nicht ratsam. Besser sind PDF-Files. Denn Word-Dokumente beinhalten viele Informationen (Meta-Daten), welche den Absender in kompromittierende Situationen bringen könnten.
- **Software:** Das Installieren unbekannter Software ist nicht ratsam. Vorsicht auch bei Freeware. Man sollte sicherstellen, dass die Quelle vertrauenswürdig ist. Es gab zuhauf Fälle, in denen Spyware in Gratisprogrammen eingebaut war. Virenschutz und alle Programme inkl. Betriebssystem sollten permanent auf dem aktuellsten Stand gehalten werden.
- **Informatik:** Vor der Entsorgung von Computern ist die Festplatte «sicher zu löschen». Dasselbe gilt vor dem Verschenken oder Verkaufen von Computern. Das Löschen oder Deaktivieren aller Benutzer-IDs von Mitarbeitern, welche das Unternehmen verlassen haben, ist höchst ratsam.
- **Recht:** Jede Unternehmung sollte darauf bestehen, dass ihre Mitarbeiter bei der Anstellung eine Vertraulichkeitsvereinbarung (Geheimhaltungs-, Sorgfalts- und Treuepflicht) unterschreiben, welche auch nach dem Austritt Gültigkeit hat.
- **Weisungen:** Es ist zudem sicherzustellen, dass alle Mitarbeitenden die internen Firmenweisungen in Bezug auf die Nutzung der Informatikmittel kennen. Eine Sicherheitspolitik erstellen zu lassen, welche die generellen Ziele der Informationssicherheit definiert, ist überaus vernünftig.
- **Sensibilisierung:** Sinnvoll ist auch die Sensibilisierung der Mitarbeitenden mit einfachen, aber wirkungsvollen Präsentationen und Publikationen. Besonders Mitarbeitende im Verkauf, im Marketing, in der Entwicklung und Filialleiter im In- und Ausland profitieren davon.
- **Zutritt:** Büroräumlichkeiten und Computerräume sind vor unbefugtem Zutritt zwingend zu schützen (Zutrittskontrolle).
- **Risiko-Analyse:** Ein lohnenswerter Ansatz ist die Durchführung einer IT-Risiko-Analyse im Unternehmen mithilfe eines Sicherheitsspezialisten. Dabei geht es darum, die Unternehmenswerte klar zu identifizieren, damit die Risiken und Gefahren richtig eingeschätzt werden können. So werden mögliche Bedrohungsszenarien mit den entsprechenden Gegenmassnahmen weit besser ersichtlich.

Fazit

Es lohnt sich sehr wohl, Zeit und Geld zu investieren, um Mitarbeitende für Sicherheitsrisiken zu sensibilisieren und klare Richtlinien aufzustellen. Denn die teuersten Firewalls und Security-Lösungen bringen nichts, wenn die Mitarbeitenden die Hintertüren durch ein falsches Verhalten für Cyberangriffe, durch die Verwendung von Dropbox etc. öffnen. Klares Ziel ist, dass die Restrisiken bekannt sind und durch die verantwortlichen Stellen akzeptiert und auch getragen werden. ■

INFORMATIONSSICHERHEIT – PRAKTISCHE TIPPS

- 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.

WOLFGANG SIDLER
ist Inhaber der SIDLER Information Security GmbH, Mitarbeiter des Datenschutzbeauftragten des Kantons Luzern, MAS in Information Security, Certified ISO 27001 Lead Auditor und Mitautor des «IT-Sicherheitshandbuches für die Praxis».