Dynamische Prozesse und die zunehmende Nutzung mobiler Geräte führen dazu, dass immer mehr Unternehmen die Kontrolle verlieren über ihre geschäftskritischen Daten. Im Gespräch mit Business&IT erläutert der **IT-Sicherheits-Experte Alexander Krist**, wie Unternehmen sensible Informationen kontrollieren und schützen können.

Alexander Krist ■ verantwortlich für den Geschäftsbereich IT-Sicherheit bei der circular Informationssysteme GmbH

INTERVIEW

> Daten außer Kontrolle

Business&IT: Herr Krist, es gibt mittlerweile viele verschiedene IT-Sicherheitsstrategien. Was unterscheidet Data Loss Prevention (DLP) und File Security von den herkömmlichen Ansätzen?
Alexander Krist: Die bei den meisten Unternehmen und Organisationen eingesetzten IT-Sicherheitsstrategien dienen vorrangig dem Schutz der Systeme und der Infrastruktur vor Eindringlingen und unautorisierten Zugriffen sowie vor Malware. Im Unterschied dazu lassen sich mit Data Loss Prevention und File Security die dynamisch wachsenden wirtschaftlichen, gesellschaftlichen und technologischen Entwicklungen berücksichtigen.

Sie setzen am höchsten Gut von Unternehmen und Behörden an: deren Daten und Informationen – und nicht an den Systemen und der Infrastruktur, die die Daten „lediglich" vorhalten, verarbeiten und verteilen. Es darf hier jedoch nicht der Eindruck entstehen, dass DLP und File Security allein als zielführend zu betrachten sind. Sie müssen vielmehr als komplementäre, aber gleichzeitig elementare Ansätze verstanden und in die vorhandene IT- und IT-Security-Strategie integriert werden.

Wie lassen sich dabei Prioritäten setzen und welcher zeitliche Rahmen sollte eingeplant werden?
Alexander Krist: Vor dem Hintergrund der aktuellen Anforderungen ist es erstens unverzichtbar, genau zu wissen, wo sich die für den Geschäfts- und Organisationsbetrieb kritischen oder vertraulichen Daten bzw. Informationen befinden. Zweitens gilt es zu definieren, wer sie auf welche Weise, auf welchen Wegen und in welchem Umfang nutzen und verarbeiten darf. Ansätze wie DLP und File Security werden dem gerecht. Beide Verfahren müssen dabei als Konzepte und Strategien, bestehend aus technischen und organisatorischen Maßnahmen, verstanden werden.

Hüten sollte man sich vor Versprechen, eine solche Zielstellung innerhalb weniger Tage und durch reine Technik erreichen zu können. Vielmehr gilt es zu erkennen, dass strategische Konzepte zunächst immer wichtiger sind als deren schnelle und rein technische Umsetzung.

Wie geht ein Unternehmen im Idealfall vor?
Alexander Krist: Das hängt wesentlich davon ab, ob und in welchem Umfang man sich bereits im Klaren darüber ist, wie hoch das Maß der Abhängigkeit von der eigenen IT und von den geschäftskritischen und vertraulichen Daten und Informationen ist. Es verhält sich also wie in der Medizin: Nur wer über eine exakte Diagnose verfügt, ist in der Lage, präzise zu handeln und gravierende Behandlungsfehler zu vermeiden. Zuständig hierfür sind eindeutig das höchste Management und die Geschäftsführung.

Große Unternehmen verfügen über Revisionsabteilungen und Stabstellen für IT-Sicherheit, zudem setzen sie Wirtschaftsprüfer und externe Fachberater ein. Daher ist es ihre Aufgabe – und nicht die der IT-Abteilungen –, den Datenfluss und die Organisationsstrukturen in allen einzelnen Unternehmensbereichen genau zu betrachten und zu untersuchen. Daraus leiten sich dann sowohl Handlungsempfehlungen als auch konkrete Anweisungen ab, etwa um Verstöße gegen das Bundesdatenschutzgesetz zu vermeiden und zahlreiche andere möglichen strafrechtlich relevanten Aspekte zu berücksichtigen.

Damit ist die Basis gelegt. Welche IT-Sicherheitsprozesse sollten anschließend angestoßen werden?
Alexander Krist: Zunächst sollten alle geschäftskritischen Daten aufgefunden, identifiziert und kategorisiert werden. Anschließend gilt es, Prozesse und Technologien für daten- und bereichsspezifische Regel-, Rollen-, Zugriffs-, Vorhaltungs- und Verarbeitungskonzepte zu entwickeln und einzuführen. Dann können Daten, Container und Verbindungen verschlüsselt und zusätzlich die gewählten Mittel auf ihre Wirksamkeit kontrolliert werden. Im anonymen Großkonzern und in öffentlichen Einrichtungen lassen sich solche Maßnahmen oft nur schwer durchführen und umsetzen, da die internen Abläufe kaum durchschaubar sind oder Mitarbeiter häufig ihre Stelle wechseln. Genau deshalb sind solche Maßnahmen aber wichtiger als im familiären Kleinbetrieb.

Viele Unternehmen statten ihre Mitarbeiter heute schon ganz selbstverständlich mit mobilen Endgeräten aus. Worauf sollten sie dabei achten und welche Schutzmaßnahmen können sie ergreifen?
Alexander Krist: WLAN, iPhone, Smartphones, Tablet-PCs oder andere mobile Einheiten und Endgeräte sind weit verbreitet. Das gilt auch für Business-Collaboration-Werkzeuge, Communities und Dienste wie Twitter, ICQ und Facebook. Sie sind zwar technisch sehr weit fortgeschritten, allerdings wird das hohe Niveau bezüglich der Sicherheitstechnologie kaum erreicht. Funktion vor Sicherheit und Vertraulichkeit ist hier also der klar erkennbare Trend.

Durch diese daher einseitig vorteilhafte Technik lässt sich manchmal schon auf einfache Weise der Gesamtbestand aller vorhandenen geschäftskritischen und vertraulichen Daten und Informationen eines Unternehmens oder einer öffentlichen Einrichtung aus dem Haus tragen. Oder jeder kann von außen ungehindert darauf zugreifen. Hinzu kommt, dass mobile Einheiten und damit auch die darauf gespeicherten Daten täglich tausendfach verloren gehen oder gestohlen werden.

Schützen können sich Unternehmen und öffentliche Einrichtungen daher nur durch mehrschichtige und ganz speziell auf den Einsatz von Mobilitätstechnologien ausgerichtete Konzepte. Kernpunkte dabei sind neben technischen Mitteln besonders organisatorische Ansätze.

Wird so der Mitarbeiter zur Bedrohung für ein Unternehmen?
Alexander Krist: Ich würde den Standpunkt umkehren: Gehen geschäftskritische Daten verloren, ist die Existenz des Unternehmens und damit jeder einzelne Arbeitsplatz gefährdet. Daher sollten Unternehmen – idealerweise gemeinsam mit den Mitarbeitern – Richtlinien entwickeln, die den Einsatz mobiler Einheiten regeln.

STATEMENT

Lothar Schulz ■
Wirtschaftsprüfer und Steuerberater beim Beratungsunternehmen AUREN in Stuttgart

Ein Fall für den Wirtschaftsprüfer

„Die meisten großen Unternehmen verfügen zwar über angemessene Sicherheitskonzepte, wenden diese jedoch nicht konsequent an – und riskieren einen geschäftsschädigenden Reputationsverlust und hohe wirtschaftliche Schäden. Damit bringen sie sich aber in eine existenzgefährdende Situation. Bei den Jahresabschlussprüfungen, die wir nach den Standards des Instituts der Wirtschaftsprüfer (IDW) durchführen, ist der Prüfungsstandard IDW PS 330 die Grundlage zur Prüfung der IT-Systeme.

Im Rahmen dieser IT-Prüfung prüfen wir auch den Bereich Datensicherheit. Die aufgedeckten Mängel und Risiken stellen wir in einem Management-Letter für den Geschäftsführer oder Aufsichtsrat zusammen. Schwerwiegende Verstöße, wie etwa gegen das Bundesdatenschutzgesetz, müssen wir in den Prüfungsbericht aufnehmen.

Die Zahl dieser Fälle ist in den letzten Jahren merklich gestiegen. Daher raten wir Großkonzernen, sich nicht nur IT-Lösungen anzuschaffen, sondern diese ganz gezielt und konsequent einzusetzen. Die Auslagerung der IT-Landschaft löst diese Schwierigkeiten nicht. Das Unternehmen bleibt verantwortlich für die Datensicherheit und muss sicherstellen, dass der externe IT-Dienstleister über eine ordnungsgemäße Organisation verfügt. Zu empfehlen ist daher eine externe Kontrolle des IT-Dienstleisters durch einen Wirtschaftsprüfer nach dem Prüfungsstandard IDW PS 951.“

STATEMENT

Michael Melzig ■
Manager Marketing Business Clients bei Fujitsu

Effektiver Schutz für Notebooks

„Nach einer gewissen Zeit steigt der Wert eines Notebooks aufgrund der installierten Software, deren Inhalten sowie der persönlichen Datensätze. Der finanzielle, wirtschaftliche Schaden durch verlorene oder gestohlene Laptops ist enorm. Laut Schätzungen beträgt er zwischen 20 und 25 Milliarden Euro pro Jahr. Und es gibt eine große Dunkelziffer von nicht angezeigten Fällen.

Dabei kostet der Rundumschutz fürs Notebook gerade mal 15 Cent am Tag. Mit unserer Technologie Advanced Theft Protection, kurz ATP, können Daten auf verlorenen oder gestohlenen Notebooks per Fernzugriff gelöscht bzw. das gesamte Notebook deaktiviert werden. Notebooks lassen sich so manipulationssicher sperren oder aus dem Verkehr ziehen, ähnlich einer Kreditkarte – ein Anruf bei der Hotline genügt. Dem Datenmissbrauch durch Unbefugte wird damit ein Riegel vorgeschoben.

Die Fernsperrung wird automatisch ausgelöst, wenn ein Nutzer beispielsweise zwei Wochen in seinem Heimnetz nicht mehr angemeldet war. Will eine fremde Person das Gerät einsetzen, wird in dem Moment, in dem das Gerät über LAN oder DSL wieder Internet-Anschluss hat, per UMTS eine Art ‚Kill-Pill' gesendet. Diese teilt dem Gerät mit, dass es jetzt deaktiviert wird. Zudem lassen sich alle Daten auf dem Gerät löschen. Mit Hilfe eines Key-Codes oder Einmal-Tokens kann das Notebook einfach wieder entsperrt und reaktiviert werden.

Das Ganze lässt sich mit einem Passwort für das Betriebssystem, einem BIOS-Passwort, einer Firewall, einer Datenverschlüsselung und einem Antivirus-Schutz entsprechend ergänzen. Physikalischer Schutz kann zum Beispiel ein Notebook-Schloss sein. Damit kann ich sicherstellen, dass das Notebook keine Beine bekommt, wenn ich in der Bahn unterwegs bin und meinen Platz verlasse."

Parallel sind regelmäßige Schulungen und die Sensibilisierung der eigenen Mitarbeiter unerlässlich. Daneben gilt es, Detailkenntnisse und Fachwissen für die IT-Abteilung aufzubauen und stets auf dem aktuellen Stand zu halten.

So lassen sich die Möglichkeiten – aber auch die Gefahren, die von den kaum noch überschaubaren Funktionsumfängen dieser Technologien ausgehen – möglichst genau kennenlernen. Zusätzlich sollten dann moderne Sicherheitstechnologien eingeführt werden.

Dabei ist es entscheidend, zu erkennen, dass gerade die Mobilitätstechnologien den Unternehmen und öffentlichen Einrichtungen eine Vielzahl neuer Geschäftsideen und -abläufe ermöglicht haben. Es geht also nicht um Verbote und Einschränkungen, sondern um den kontrollierten Einsatz mobiler Einheiten.

Wie lässt sich dieser realisieren?

Alexander Krist: Als unverzichtbar zeigen sich hier ebenfalls die Ansätze von DLP und File Security, die, verbunden mit mehrstufigen Berechtigungs- und Authentifizierungsmechanismen, den größten Nutzen aufweisen. Gemeinsam eingesetzt, erlauben sie, granular zu kontrollieren und zu steuern, welche der Daten und Informationen gelesen, verarbeitet, kopiert oder gelöscht werden dürfen. Zudem ist es wichtig, alle Daten, Container und die gesamten mobilen Einheiten – einschließlich aller Verbindungswege, über welche die Daten und Informationen übertragen werden – mit höchstmöglichem Standard zu verschlüsseln.

Als weitere Maßnahmen sind spezielle auf den Mobility-Bereich ausgerichtete Anti-Malware-Lösungen notwendig. Sie bekämpfen wirksam Malcodes, die gezielt und vorsätzlich dazu genutzt werden, in Systeme einzudringen, sie auszuspionieren und die Daten missbräuchlich zu nutzen. Unverzichtbar sind zusätzlich starke Authentifizierungsverfahren – sowohl für die Benutzer als auch für die mobilen Systeme.

Welche Werkzeuge gibt es dazu?

Alexander Krist: Für die Authentifizierung und Autorisierung von Benutzerzugriffen müssen Einmalpasswort-Systeme als Mindeststandard gelten. Noch wirksamer sind alternativ oder zusätzlich eingesetzte Benutzer- und Gerätezertifikate, verbunden mit einer eigenen oder einer öffentlichen Certificate Authority (CA).

Eine weitere empfehlenswerte Komplementärmaßnahme stellen sogenannte Network-Admission-Control-Lösungen dar. Sie schützen die Netzwerke sowie die darin verarbeiteten Daten und Informationen vor dem Zugriff unautorisierter oder nicht den Unternehmensrichtlinien entsprechender mobiler Systeme, die zum Beispiel durch Infektion ausgelöstes verdächtiges Verhalten zeigen oder nicht über aktuelle Release-Stände und Security-Patches verfügen. *[rm]*