

Schutz vor Datenverlust muss breit angelegt werden

Datenschutz, Bank-Kundendaten und Vertraulichkeit. Wir wissen um die Wichtigkeit der Informationen. Und meist ist klar, welche Daten vor einem Verlust oder Abfluss («Leakage») geschützt werden sollten. Aber, was machen wir dagegen? Oft fehlt sogar der Überblick, wie ein Datenverlust passieren kann und was eine gute Abhilfe wäre.

VON ZRINKA MASLIC

Datenverlust kann ein ganzes Spektrum von Gründen haben. Zu den klassischen gehören sicherlich versehentlich gelöschte Daten und «gecrashte» Systeme – häufig in Kombination mit nicht funktionierenden Backups. Hierbei ist der Datenverlust tatsächlich wörtlich zu interpretieren, da die Daten faktisch niemandem mehr zur Verfügung stehen. Wenn sie zeitgerecht wieder aufbereitet werden können, hat ein solcher Verlust oft nur den Nachteil, dass er viele Arbeitsstunden für das Recovery gekostet hat.

Datenverlust oder Datenabfluss?

Anders sieht es aus, wenn der Datenverlust eigentlich ein Datenabfluss ist. In diesem Fall sind die Daten vielleicht nach wie vor im Zugriff der eigenen Firma, jedoch sind nun auch andere, vielleicht unbekannte Personen im Besitz der Daten. Solche Informationslecks entstehen häufig unabsichtlich. Zum Beispiel werden immer wieder E-Mails versehentlich an die falschen Empfänger verschickt und Informationen landen somit in falschen Händen. Ähnliche Effekte ha-

ben verlorene oder gestohlene Notebooks, USB-Sticks, CDs usw. Wo keine Gewinnabsichten hinter dem Verlust der Daten stecken, sind die Auswirkungen der Verluste sehr schwierig einzuschätzen.

Mit hohen Kosten und Reputationsverlusten ist zu rechnen, wenn der Verlust der Daten öffentlich gemacht wird oder sogar gegen die Firma verwendet wird. All die Schlagzeilen aus Grossbritannien bezüglich verlorener oder fälschlicherweise veröffentlichter Daten haben das Vertrauen in die Verwaltungseinrichtungen der Briten sicher nicht gerade gefördert. Für eine private Firma können solche Vorfälle desaströs sein. Erpressungen gegen Finanzinstitute, Diebstahl geistigen Eigentums oder Wirtschaftsspionage sind heutzutage leider tägliche Erscheinungen.

Zwischen Kriminalität und Ignoranz

Grundsätzlich kann Datenverlust auf zwei Ebenen passieren: absichtlich oder unabsichtlich. Absichtlicher Datendiebstahl mit kriminellem Hintergrund bildet den Extremfall der einen Ebene, während auf Unwissenheit

beruhende Fehlhandlungen den Extremfall der zweiten Ebene bilden (siehe Grafik).

Die ideale Situation in einer Firma besteht, wenn Technik und Organisation für die Menschen lebbar sind. Dafür benötigt es gut geschulte und über Informationssicherheit aufgeklärte, loyale und zufriedene Mitarbeiter. Ein umfassendes und klares Regelwerk (Policies) bildet den Rahmen für den Umgang mit Firmeneigentum. Eine reibungslos und gut strukturierte Organisation der Prozesse und Geschäftsbereiche sorgt für die praktische Umsetzung. Eine moderne IT-Infrastruktur vermag die Prozesse und formulierten Regelwerke technisch zu stützen. Unter solch idealen Bedingungen gehören Datenverluste zu den seltenen und eher unwahrscheinlichen Vorfällen.

Viele Menschen arbeiten allerdings in Umgebungen, die mehr oder weniger von der Idealsituation abweichen. Verschiedene Faktoren können zusammenkommen und für eine schwierige, sogar gefährliche Situation sorgen: Mangelhafte Prozesse provozieren die Mitarbeiter dazu, Regeln zu umgehen und heikle «Ab-

kürzungen» zu nehmen. Mängel in der Organisation führen dazu, dass Verantwortungen und Zuständigkeiten unklar sind, was oft Verzögerungen mit sich bringt. Mangelhafte Infrastruktur und Werkzeuge veranlassen Mitarbeiter zur Umgehung von Sicherheitsmassnahmen.

Je grösser die Diskrepanz zur Idealsituation ist, desto eher entsteht eine Extremsituation, in der ein Datenverlust zu einer hohen Wahrscheinlichkeit wird.

Viele Unternehmen handeln fahrlässig

Treffen Umstände auf der «kriminellen» Seite (siehe Grafik) zu, sind Mitarbeiter empfänglich für fremde Angebote wie z.B. neue Arbeitsstellen oder, weit schlimmer, Bestechungsgelder. Unzufriedene Mitarbeiter verspüren kein besonderes Pflichtgefühl gegenüber ihrer Firma und könnten auf solche Angebote eingehen. Datenverluste passieren dann häufig in einem recht unauffälligen Bereich: Häufig nehmen Mitarbeiter die für ihre Arbeit wichtigen Informationen mit und bringen sie in ihrer neuen Firma ein. Oft sind dies «harmlose» In-



DIE ELEMENTE EINER WIRKSAMEN DLP-STRATEGIE

1. Datenklassifizierung: Eine exakte und klare Datenklassifizierung ermöglicht die Erkennung sensibler Daten.

2. Policies: Richtlinien bilden die Grundlage zur Handhabung der Daten, indem sie den Datenklassen Handlungsanweisungen zuordnen (z.B.: Wie werden welche Datenklassen erkennbar gemacht, wann muss welche Verschlüsselung eingesetzt werden, wann muss wie authentifiziert werden?)

3. Prozesse: Plausible und lückenlose Prozesse führen den Benutzer nicht nur während Standardsituationen, sondern auch in Ausnahme- und Notsituationen durch die Ver- und Bearbeitung der Daten.

4. Filter-Systeme: IT-Security-Infrastruktur, welche «positiv» filtert und den Benutzerkomfort hoch behält, dient sowohl dem Schutz der Daten als auch der Förderung der Mitarbeiterakzeptanz gegenüber Sicherheitstechnologien. Filter sollten vor allem «zulassen» und nicht «verhindern» – eine Blockade durch einen Filter sollte klar als die Verhinderung von Negativem empfunden werden (z.B. gelten Viren-, Spam-, Phishing-Filter als positive Filter).

5. Zugriffskontrollen: Komfortable Authentifizierungssysteme setzen Zugriffs-Policies in die Realität um, ohne vom Benutzer als aufwendig und lästig empfunden zu werden (z.B. Enter-

prise Single Sign On, SmartCards, usw.).

6. Workflow-Systeme: Prozesse und Kontrollpunkte können durch Workflow-Systeme gestützt durchgesetzt und effizient abgewickelt werden. Speziell für den Bereich DLP gibt es Systeme, welche auf Weichenstellungen beim Datentransport ausgerichtet sind.

7. Logging/Monitoring: Die nachvollziehbare Aufzeichnung und Erkennung von Vorgängen im Zusammenhang mit Datenzugriffen ist nicht nur eine Vorgabe von vielen Auditoren, sondern bildet eine wichtige Voraussetzung bei der Analyse von Fehlern oder Missbräuchen zu deren künftiger Verhinderung.

8. Schwachstellen-Management: Ein gutes Schwachstellen-Management ermöglicht die frühzeitige Erkennung und Eliminierung von wahrscheinlichen Angriffszielen (wird am besten mit dem Risk-Management und dem Betrieb/Patch-Management kombiniert).

9. Sicherheitskultur: Eine Sicherheitskultur, welche die Werte der Firma auf die Mitarbeiter zugeschnitten portiert, hat grössere Chancen, akzeptiert und gelebt zu werden.

10. Mitarbeiter-Schulungen: Gut informierte bzw. geschulte Mitarbeiter sind organisatorischen und technischen Vorgaben gegenüber positiver eingestellt und leben die Sicherheitskultur ihrer Firma aktiv vor.

formationen wie eine Kundenliste oder Dokumentationen. Kritisch wird es, wenn es sich um Informationen aus dem Kerngeschäft der Firma handelt, wie z.B. Produktbaupläne eines Industriebetriebes, Datenbanken eines Marktforschers usw.

Beim anderen Extrem, der Unwissenheit, sind Angebote nicht unbedingt ein Lockmittel, mit dem Mitarbeiter zur Herausgabe von Daten geködert werden könnten. Jedoch könnten allgemeine Gleichgültigkeit und Ignoranz zu ähnlichen Effekten führen. Ungepatchte Systeme, die Angreifern Tür und Tor zu den Firmendaten öffnen, Zugriffsregeln, die keine Rücksicht auf das «Need to know»-Prinzip nehmen, gehören leider zu täglich anzutreffenden Umständen in vielen Firmen. Auch das oft gepriesene «organisierte Chaos», welches Mitarbeitern ein kreatives Umfeld und viel Eigenverantwortung bietet, kann in ein sehr

ungesundes Wirrwarr von Nichtzuständigkeiten und Unterlassungen umkippen. Dies wiederum kann durchaus negative Auswirkungen auf den Umgang mit Firmeneigentum haben – vielleicht sogar mit besten Absichten der Mitarbeiter.

DLP – ein Teil der Informationssicherheit

Data Loss Prevention oder kurz DLP ist ein Spezialgebiet innerhalb des klassischen Risk- und Information-Security-Managements. Es hält an den gleichen Vorgaben, Idealen und Prinzipien fest und konzentriert sich dabei spezifisch auf die Verhinderung absichtlichen Datenabflusses bzw. den Schutz vor versehentlicher Offenlegung vertraulicher oder sensibler Informationen. Man kann DLP innerhalb der Information-Security durchaus als die Konzentration auf das Wesentliche verstehen – zumal Wirtschaft und Verwaltungen kaum

mehr Daten verarbeiten, die nicht digital vorhanden wären.

Das Kernziel von DLP ist es, digitale Daten in den für sie angedachten Räumen zu behalten. Eine der Herausforderungen besteht darin, dass digitale Daten auch digitale Räume belegen, bestehend aus Netzwerkstrukturen, Servern und Applikationen. Mit der Tendenz zu Cloud Computing und SaaS (Software as a Service) verschwinden heute sogar die digitalen Grenzen, welche wir vor nicht allzu langer Zeit noch sehr komfortabel definieren konnten.

Wie in der physischen Welt muss auch die digitale Welt darauf ausgelegt werden, den Schutz der Daten zu garantieren. Genau wie in der physischen Welt wird dies auf verschiedenen Ebenen angestrebt. Eine Strategie, welche dem Schutz Ihrer Daten dient und deren Abfluss aus Ihrer Firma verhindern soll, muss von Beginn an breit angelegt sein und neben technischen Massnahmen auch organisatorische beinhalten.

Nicht zuletzt ist die Miteinbeziehung der Menschen als Mitarbeiter und Bearbeiter der Daten einer der wichtigsten Punkte jeder DLP-Strategie.

Technische Mittel allein reichen nicht

Um die digital vorhandenen Werte eines Unternehmens vor Verlust oder Diebstahl zu schützen, sind breit angelegte Strategien nötig. Ein Datendiebstahl kann kaum alleine durch technische Mittel verhindert werden. Wer Daten stehlen will, wird immer Mittel und Wege finden, dies zu tun. Eine gute DLP-Strategie, welche bei der Definition der technischen und organisatorischen Massnahmen immer auch die Mitarbeiter mit einbezieht und zudem eine offene und gesunde Unternehmens- respektive Sicherheitskultur pflegt, senkt die Wahrscheinlichkeit von Datenverlusten. ■■■■

Zrinka Maslic ist Head Technology & Engineering bei ISPIN AG in 8303 Bassersdorf.
www.ispin.ch

Anzeige