Alle Schotten dicht

Ein effizientes DLP-Konzept schützt vor dem Verlust sensibler Daten

In vielen Unternehmen und Behörden wird täglich mit Daten gearbeitet, die besonderen Schutz benötigen. Ungewollter Datenabfluss kann von außen, aber auch von innen ausgelöst werden. Deshalb müssen sämtliche potenziellen Datenlecks identifiziert, überwacht und abgesichert werden.

Daten sind der Rohstoff des 21. Jahrhunderts – und wecken Begehrlichkeiten. Längst hat sich eine Szene im Darknet etabliert, die gegen Zahlung den gezielten Datendiebstahl verspricht. Und anders als bei gestohlenen Autos lassen sich die Daten gleich mehrfach verkaufen – der Profit steigt. Die Gesetzgebung mag ausreichend sein, doch die Strafverfolgung ist nicht in der Lage, allen Delikten in allen Ländern nachzugehen. Der Schaden von einmal gestohlenen Daten kann, wenn diese bereits verkauft oder weitergegeben sind, nicht mehr geheilt werden, denn die Daten sind dann nicht mehr einzufangen.

Das einzig sinnhafte Konzept ist es deshalb, seine wichtigsten Daten selbst zu schützen. Sind die kritischen Daten identifiziert, gilt es, den adäquaten Schutz umzusetzen, denn nicht bei allen Daten gelten die gleichen Schutzziele. Manche müssen vor Innentätern geschützt werden, bei manchen ist es sinnvoll, die eigenen IT-Mitarbeiter vor dem Verdacht der unerlaubten Kenntnisnahme zu schützen. Mechanismen der Data Leakage/Loss Prevention (DLP), helfen dabei, ungewünschten Datenabfluss zu verhindern. Das eigene Risikomanagement definiert dann, wie robust der Schutzmechanismus jeweils sein muss.

Die gesamte Handlungskette sichern

Auch die Handlungskette bei der Datennutzung ist nur so stark wie ihr schwächstes Glied. Im ersten Schritt werden die Daten generiert. Im nächsten Schritt wird über Services, Netzwerke, Anwendungen oder Apps auf die Daten zugegriffen, um sie dem Nutzer zu präsentieren, der sie dann wiederum mithilfe anderer Anwendungen weiterverarbeitet, speichert, druckt, verschickt usw. Hat der Nutzer beliebige Freiheit bei der Verarbeitung, ist prinzipiell davon auszugehen, dass sich die Daten später elektronisch nicht wiedererkennen lassen, da sie verschlüsselt bzw. zu Bildinformationen oder in andere Formate gewandelt wurden. Für die Ziele der Integrität und Vertraulichkeit gilt es also, die gesamte Handlungskette so zu organisieren, dass ein adäquater Schutz in allen Lebenslagen für die Daten besteht. Das klingt noch relativ einfach, wenn man die wirklich sensiblen Daten in geeignet geschützten Datenräumen unterbringt und der Schutz mit hoher Robustheit durchgesetzt wird. Zur Absicherung der gesamten Handlungskette muss allerdings der vollständige Lebenszyklus betrachtet werden.

Eine erste Schwachstelle ist das Identity and Access Management (IAM). Angriffe auf die Passworteingabe mittels „über die Schulter schauen“ und Keylogger sind bekannt und können mit guten Awareness-Maßnahmen (auch gegen Kameras) und einigen Endpoint-Security-Lösungen verhindert werden. Der Angriff auf den Deutschen Bundestag im Jahr 2015 hat aber gezeigt, dass auch über andere Angriffe wie PassTheHash und Mimikatz die Identität eines Anwenders gestohlen werden kann, ohne dass man dessen Passwort und Username benötigt. Das Problem des Identitätsdiebstahls ist also viel komplexer, als dem Anwender seinen Besitz (Smartcard oder Zugangstoken) und sein Wissen (Passwort/PIN) zu stehlen.

Zugangskontrollen prüfen

Viele Sicherheitsberater gehen heute davon aus, dass man nicht jede Umgebung „sauber“ halten kann und in manche IT-Umgebungen wenig Vertrauen setzen sollte – insbesondere in solche, die über viele Services notwendigerweise mit dem Internet verbunden sind und dazu auch Nutzdaten austauschen. Wird dieselbe Kennung für diese unsicheren Umgebungen und gleichzeitig (ohne Zusatzschutz) für die sicheren Datenräume verwendet, kann von Sicherheit nicht mehr die Rede sein. Die Eingabe eines mehrfach nutzbaren Passwortes auf der Tastatur eines mobilen Endgerätes potenziert das Risiko. Wenn die Identität gestohlen ist, greifen alle nachfolgenden Sicherheitsmaßnahmen, die auf den Rechten Einzelner beruhen nicht mehr. Gleiches gilt natürlich für die unberechtigte Nutzung von Benutzerrechten durch schadhafte Anwendungen auf einem IT-System, mit dem der Anwender tatsächlich arbeitet.

Einem Benutzer sind aber meist mehrere Kennungen für unterschiedliche Datenräume nicht zuzumuten. Wichtig ist hier also die Vertrauensstellung der einzelnen Systeme untereinander. Ein System mit hoher Vertrauensstellung kann ein automatisches Login in ein niedrigeres System durchführen – umgekehrt darf das nicht passieren. Prinzipiell gilt also, dass die Tastatur zur Eingabe eines mehrfach verwendbaren Passwortes im Sicherheitsraum der genutzten Daten und Services liegen muss. Um lokale Angriffe zu vermeiden, müssen entsprechende Vorkehrungen bei der Kommunikation der Tastatureingaben getroffen werden.

Häufige Fehler bei DLP-Projekten

DLP-Projekte benötigen sehr viel Detailverständnis. Heutzutage sind IT-Projekte aber dazu gezwungen, bereits nach kurzer Zeit einen sichtbaren Nutzen zu erbringen und nicht als permanentes Groschengrab nur Ressourcen zu verbrauchen. Schnelle Erfolge lassen sich bei DLP-Projekten einfach erzielen: Das Monitoring der potenziellen Leckage-Punkte führt dazu, dass die notwendigen Schutzmaßnahmen erkannt und priorisiert werden können, ohne dabei den Betrieb zu behindern. Leckage-Punkte sind etwa Kommunikationsbeziehungen nach außen, wie E-Mail oder Browser-Upload, mobile Datenträger und spontane Kommunikation über Devices wie Bluetooth, WiFi etc., aber auch

Ausdrucke, Fotos von Bildschirmen und Informationen, die durch das „über die Schulter schauen“ gewonnen werden.

Wer zuerst versucht, alle vorhandenen Daten nach deren Kritikalität zu markieren – und dafür viel Zeit und Energie aufbringt – wird lange auf positive Resultate warten müssen. Das eigentliche Ziel, Daten vor unerlaubtem Abfluss zu schützen, wird man dann spät oder gar nicht mehr erreichen. Ignoriert man zusätzlich die systembedingten Ungenauigkeiten durch die unterschiedlichen Repräsentationen der gleichen Information (Sprachen, Sonderzeichen, OCR/Bild von Text, Formatierungen, Steganografie, Covert Channels …) in der Klassifikationsphase, werden viele „falsche Fehler“ (false positives und false negatives) dazu führen, dass man im Betrieb entweder häufig nachbessert und hohe administrative Kosten generiert oder die echten Schutzkriterien so lax einstellt, dass das Ergebnis den Aufwand nicht mehr wert ist.

Fallen identifizieren

Liegt der Fokus nur auf dem internen Datenabfluss, verstellt man den Blick auf Angriffe von außen, die erst im Ergebnis zum unerwünschten Datenabfluss führen. Häufig wird über Angriffe auf die Schwachstellen von Standardanwendungen (Browser-Exploit) oder Standardformate (Flash, PDF-Exploit) erst der unerwünschte Datenkanal nach außen geöffnet, der dann aufgrund stenografischer Verfahren nicht mehr erkannt werden kann. Der Angriff kommt aber von außen, weshalb es zu einer wesentlichen Aufgabe des DLP gehört, den „Import von schädlichen ausführbaren Objekten“ zu kontrollieren oder ganz zu verbieten, z.B. Javaskript in PDF, DLL-Download über Browser etc. Es ist also zwingend notwendig, ein Inventar aller zur Ausführung kommenden Programme zu halten und dieses sukzessive nach der Kritikalität für DLP zu bewerten. Dieser Schritt ist schon darum wertvoll, weil man alle Programme, Skripte, Makros etc. kennenlernt, die bisher nicht im Softwarekatalog oder dem offiziellen Inventar standen.

Best Practice für DLP

Einfache, weil im Betrieb unkritische Sicherheitsmaßnahmen (Quick Wins) sind zuerst an der Reihe. Das heißt, Maßnahmen wie Benutzersensibilisierung, Monitoring, Risikoinventarisierung und Alerting stellen die ersten Schritte dar und erlauben es, die Kritikalitätseinschätzung iterativ zu verfeinern. Die zyklische Untersuchung der statistischen Auswertung zeigt die realen Risiken und praktische Verstöße gegen die bestehenden Vorschriften auf. Bereits nach dieser Phase, die mit wenigen Arbeitsstunden erledigt ist, kann man klare Antworten auf die drängenden Fragen „Wie sicher sind wir?“ und „Wo ist unser dringendster Bedarf?“ geben. Das bildet die Grundlage für die regelmäßige Verfeinerung der technischen Sicherheitsmaßnahmen. Je nachdem identifizierten Datenmaterial, der verwendeten Applikation, dem Netzwerk, dem Datenträger, dem handelnden Benutzer und weiteren Parametern werden dann folgende Maßnahmen nahegelegt oder sogar erzwungen:

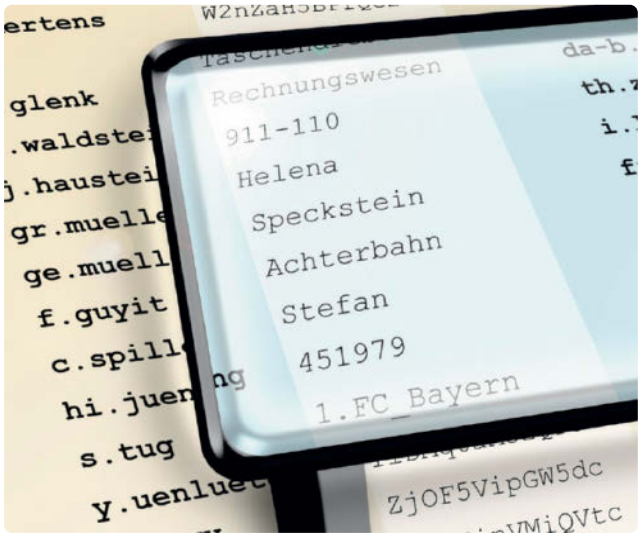
Bewusstseins- und wissensbildende *Informationen* über das konkret identifizierte Risiko an den Anwender in Echtzeit, evtl. mit elektronischer Willenserklärung für einen juristisch nachhaltigen Haftungsübergang; *Verschlüsselung* mit Unternehmensschlüssel oder persönlichem Schlüssel, je nachdem, ob der Anwender das Recht haben soll, diese Daten eigenständig, z.B. auf seinem privaten Rechner, zu nutzen (BYOD); revisionssichere *Beweiserhebung* und evtl. Alerting bei kritischen Aktionen; letztlich auch eine *Blockade*.

Bei der Wahl eines technischen Produktes ist es wesentlich, dass eigene algorithmische Prüfungen und solche von Drittprogrammen eingebunden werden können, sodass eine Sequenz von Prüfungen nach unterschiedlichen Kriterien entsteht. Mittelfristig sollte man die sensibelsten Daten in sicheren Datenräumen (Private Data Room) mit einfachen Richtlinien (Read up – No write down) sammeln und diese sicheren Datenräume nur über virtuelle Mechanismen einbinden.

Eine rein organisatorische Lösung ist nicht ausreichend, da der Mitarbeiter den Abfluss der Information oft gar nicht erkennen kann, z. B. wenn dieser durch Schadcode als Upload über den Browser stattfindet. Vielmehr muss zumindest ein Teil der Sicherheitsrichtlinie technisch umgesetzt werden. IT-Sicherheit gegen den Anwender durchzusetzen, ist sehr teuer oder gar unmöglich, deshalb sollten die Maßnahmen immer für die effiziente Abwicklung des Anwendungsfalls und damit für den Anwender – nicht gegen ihn – getroffen werden. Auch für das Umsetzen der Anforderungen aus den rechtlichen Auflagen, z. B. dem Datenschutz, hat sich ein software-gestütztes Risikomanagement bewährt. Die Ergebnisse der Überwachung der Leckage-Punkte bilden dann die Grundlage für das DLP-Risikomanagement und fließen in ein immer detaillierteres DLP-Konzept ein.

Verstöße vermeiden

Audit und revisionssichere Protokollierung bestimmter Aktivitäten dienen dazu, bestimmte Ereignisse für eine spätere Auswertung abzuspeichern, ohne dass diese Daten im Nachhinein modifiziert werden können. Die Audit-Funktionalität meldet in Echtzeit Sicherheitsvorfälle und ermöglicht so eine Alarmierung der Verantwortlichen und das Nachjustieren der technischen Richtlinien. Entsprechend der jeweiligen lokalen Gesetze sind die Log-Daten entweder völlig ohne Anwenderdaten zu erheben oder anonym bzw. pseudonymisiert zu speichern. Die Protokollierung von Risiken hat nichts mit der Überwachung von Anwendern zu tun, sondern eher mit dem Schutz der Anwender vor unsichtbaren Angriffen, die später so aussehen können, als wäre der Mitarbeiter selbst Innentäter.



Quelle: itWatch

Ausdrucke können sensible Daten enthalten.

Bei (unbewusst) versuchten Verstößen gegen die definierten Regeln bieten DLP-Tools ereignisabhängig abgestufte Reaktionsmöglichkeiten. Dazu gehören beispielsweise: die Anzeige eines *Hinweises* für den Benutzer, dass die geplante Transaktion gegen das Regelwerk verstoßen würde; die Abfrage einer expliziten *Zustimmung* des Benutzers, z. B. zur Protokollierung der Tätigkeiten; die *Freigabe* der Aktion unter bestimmten Auflagen; die Abfrage von *Gründen* für die Aktion; die *Blockade* der Aktion; die Protokollierung sowie die Freigabe durch *Dritte*, etwa einen Administrator oder Vorgesetzten.

DLP bei mobilen Daten

Das lokale Sammeln im Abfall wird bei Flash-Datenträgern noch kritischer, da diese den verwendeten Datenbereich nicht notwendigerweise wieder aufzeigen, sondern lebensverlängernde Maßnahmen durch versteckte Datenspeicher implementieren. Ein Verschlüsseln am Platz ist hier nicht möglich. Auf den ersten Blick genügt es, sensible Daten nur auf selbstverschlüsselnder Hardware zu speichern. Doch auch mit Datenträgern, die den gesamten zu speichernden Datenstrom verschlüsseln, löst man das DLP-Problem nur teilweise, denn der einfache und weit verbreitete Angriff mittels USB-Dumper oder erweiterten Werkzeugen bleibt hierbei wirksam. Bei der Verwendung eines vermeintlich sicheren Datenträgers auf einem jedoch unsicheren Fremdsystem kann der ganze Datenträger mittels PIN oder biometrischer Verfahren geöffnet werden.

Jede Anwendung auf dem Rechner kann alle Daten lesen, weil der Datenträger transparent entschlüsselt wird. So liest der USB-Dumper, weil er eine Anwendung auf dem Rechner ist, ohne Kenntnis des Nutzers alle Dateien aus und erhält diese im Klartext, denn der Datenträger ist ja geöffnet. Zudem wird gelegentlich übersehen, dass ein sicheres Löschen immer abhängig von der konkreten Bauart des Datenträgers ist und zudem in die Rechtestruktur eingebettet werden muss. Nicht zuletzt sind alle auf einem fremden System entstehenden temporären Dateien zu berücksichtigen, sodass diese nicht auf dem Fremdsystem verbleiben.

Dies alles sind Themenfelder, die man nicht dem Anwender überlassen kann, weil dieser sich ja auf sein Business und nicht das IT-Umfeld konzentrieren soll. Ein entsprechendes Sicherheitsprodukt muss daher automatisch temporäre Information auf dem Drittsystem löschen. Für das sichere Löschen auf mobilen Datenträgern gilt es, entsprechend der Eigenschaften des Datenträgers (Flash, magnetische oder optische Datenträger, Multiple Write oder WORM etc.) den richtigen Algorithmus auszuwählen, sodass zu schützenden Daten auch mit forensischen Werkzeugen nicht mehr rekonstruierbar sind. Bei „Write-Once-Read-Many"-Datenträgern (WORM) geht dies beispielsweise nur über den Hinweis, dass der Datenträger insgesamt einer physischen Zerstörung zugeführt werden muss – idealerweise informiert man in dieser Nachricht dann auch gleich über den Standort eines geeigneten Vernichtungsapparates oder liefert einen Link auf den vorgesehenen Vernichtungsprozess. Das sichere Formatieren vorhandener Datenträger (auch wiederbeschreibbarer optischer Medien) muss ebenfalls gewährleistet sein. Alle Verfahren sollten zudem internationalen Standards und Auflagen beziehungsweise den Empfehlungen des BSI folgen.

Auch wenn alle klassischen Schnittstellen gesichert sind, stellen Drucker häufig noch einen weiteren Leckage-Punkt dar. Ausdrucke las-

sen sich, wenn sie nicht geeignet kenntlich gemacht sind, einfach in andere Papiere oder Unterlagen integrieren und mitnehmen. Für die Sicherheitskontrolle am Ausgang ist es kaum möglich, die Kritikalität von Papieren einzuschätzen. Ohne fundierte Beweislage führt ein Vorfall schnell zu einem Generalverdacht auf alle Personen mit Leserecht und bringt dadurch unnötigen Unfrieden in die Organisation. Diese Sicherheitsherausforderung lässt sich nicht mit einem allgemeinen Druckverbot für bestimmte unternehmenskritische Dokumente lösen.

Eine adäquate Antwort darauf bietet nur ein Schutzkonzept, das die Sensitivität eines Dokuments in Echtzeit feststellt und entsprechend dem Schutzbedarf definiert, wer diese Information wann auf welchem Drucker wie ausdrucken darf und gegebenenfalls, welche Daten über die Umstände des Ausdrucks vom Anwender vor dem Ausdruck zu erfragen sind. Solche Informationen sollten dann auch auf dem Ausdruck mittels eines Wasserzeichens festgehalten und in einem revisionssicheren, elektronischen Archiv protokolliert werden. Die Angaben auf dem Dokument sind dabei notwendig, um den ermittelten Sensitivitätsgrad auch über den Medienbruch hinweg festzuhalten und in gedruckter Form dauerhaft mit der Information zu koppeln. Das Wasserzeichen kann maschinenlesbar oder lesbar für Menschen sein, je nachdem was bezweckt wird.

Sicherheitslösungen, die das Drucken sensitiver Daten kontrollieren, müssen naturgemäß alle Druckvorgänge überwachen und immer dort eingreifen, wo System oder Anwender die zu druckenden Informationen als kritisch einstufen. Für neu erstellte oder noch nicht klassifizierte Dokumente sollte unmittelbar eine Einstufung (ggf. durch den Anwender) erzwungen werden. Diese ermittelten oder in Echtzeit vom Anwender hinzugefügten Daten sollten zudem – zusammen mit dem vollständigen Inhalt des Ausdrucks jederzeit wiederherstellbar – revisionssicher abgelegt werden. Erst so ist dokumentiert, wer wann und warum welches Dokument mit welchem Inhalt in welcher Stückzahl und über welchen Drucker ausgegeben hat – und auch Auflagen der Langzeitarchivierung werden gleich mit erfüllt.

Fazit

Bei der richtigen Wahl des Vorgehensmodells und der eingesetzten Lösung(en) kann man auch bei dem komplexen Thema DLP Investitionsschutz, Skalierbarkeit, Zukunftsfähigkeit und Kosteneffizienz im Betrieb mit einem schnellen Projekterfolg kombinieren. Am besten natürlich technisch unterstützt mit einem Werkzeug, welches das Risikomanagement und die Schutzfunktionen in einem Produkt anbietet und dadurch die Lebenszyklen von Risiken und Daten vollständig abbildet. Wer seine sensibelsten Daten in sicheren Datenräumen segmentiert und zudem wirklich alle Leckage-Punkte und alle Stadien des Informations-Lifecycle berücksichtigt, besitzt ein ganzheitliches DLP-Konzept, und verhindert nachhaltig eine Gefährdung des Unternehmenskapitals, das in Form von gespeichertem Wissen und Informationen vorliegt.

Ramon Mörl,
Geschäftsführer itWatch GmbH