Nr. 3, Juli 2012

<kes>

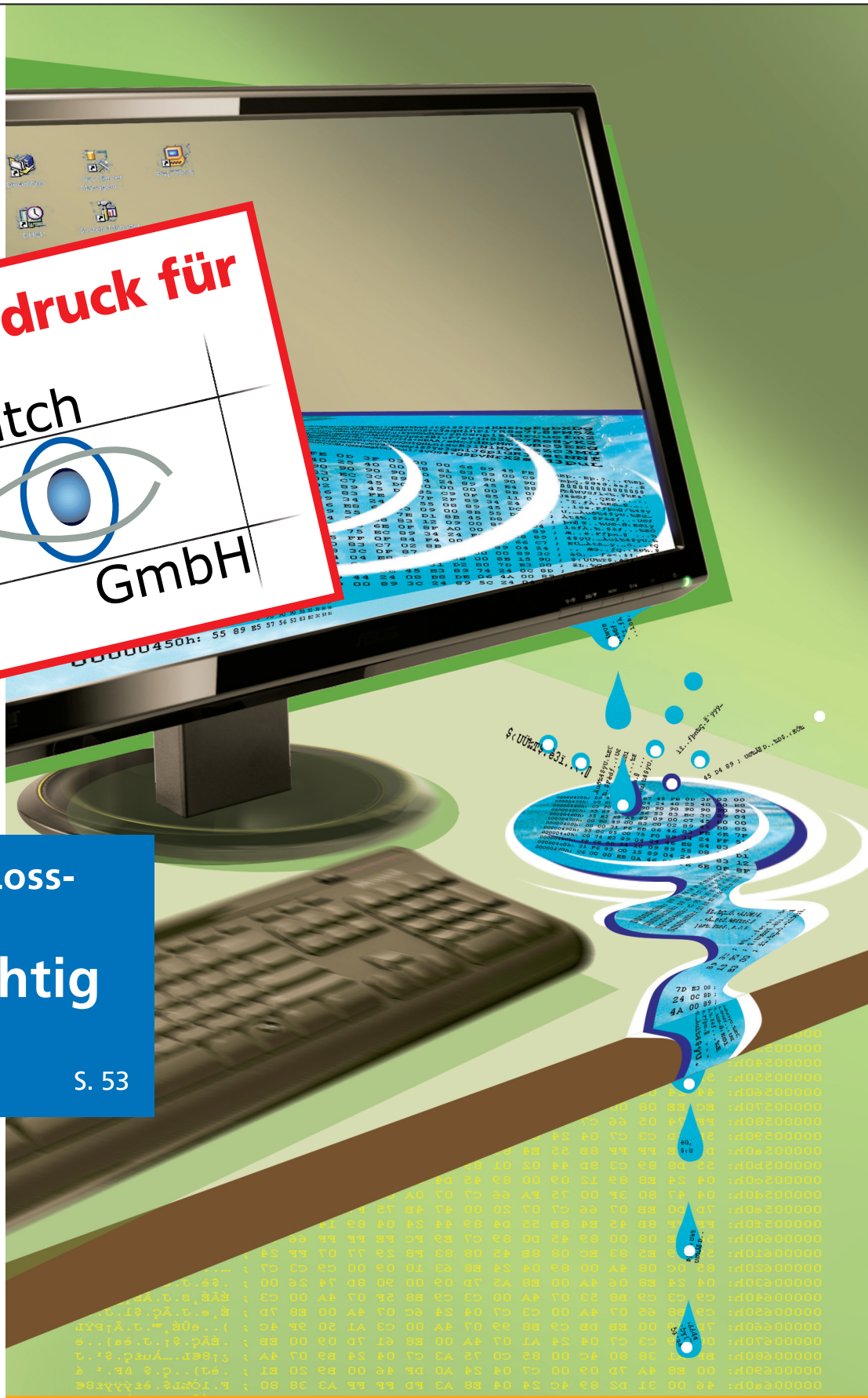
Die Zeitschrift für Informations-Sicherheit

ISSN 1611-440X

BSI Forum

offizielles Organ des BSI

Bundesamt für Sicherheit in der Informationstechnik



Sonderdruck für itWatch GmbH

Data-Leakage-/Loss-Prevention: Systeme richtig abdichten

S. 53

SecuMedia

Das etwas andere Risiko: **Burnout in der Security** S. 11

DLP zu Ende gedacht

Data-Leakage-/Loss-Prevention auch beim Drucken und Löschen

Daten sind *der* Rohstoff des 21. Jahrhunderts – auch auf dem Schwarzmarkt. Mechanismen der Data-Leakage-/Loss-Prevention (DLP), die unerlaubten oder ungewünschten Abfluss von Daten verhindern sollen, müssen neben etablierten Kanälen auch den Datenfluss über Drucker sowie vermeintlich gelöschte Information betrachten, um einen umfassenden Schutz zu gewährleisten.

Von Ramon Mörl, München

Wirtschaftsspionage wird heute elektronisch betrieben – entsprechende Angriffe erreichen Unternehmen und ihre Mitarbeiter über Standardsituationen, beispielsweise als PDF-Dateien oder den Browser. Ihr Ziel: Wichtige Daten unbemerkt „nach Draußen" zu transportieren. Eine gute Informationssicherheit lässt sich heute nur erreichen, wenn man sowohl versucht, eingehende Angriffe zu blockieren als auch – in zweiter Verteidigungslinie – unerwünschte Datentransfers zu verhindern.

Dazu gehören der Perimeterschutz mit einem guten Firewallsystem und aktuelle Netzwerksicherheitslösungen, wie beispielsweise das Kapseln sensitiver Netze in eigene LANs oder VLANs. Doch auch „Leckagepunkte" direkt auf den Endgeräten oder innerhalb virtueller Benutzersitzungen müssen gesichert werden. Aufgabe der DLP-Lösungen ist es letztlich, eine virtuelle Hülle um Betriebssysteme und Netze zu legen und für jedes Einfallstor und jeden Ausgabekanal einen adäquaten Steuerungsmechanismus bereitzustellen.

Dabei haben es sowohl die Forderung, alle Kanäle zu erfassen, als auch der Begriff des „adäquaten Steuerungsmechanismus" in sich: Einerseits bleiben häufig unbeachtete Restrisiken, weil etwa Druckdaten sowie temporäre oder vermeintlich gelöschte Informationen ungeschützt sind. Und andererseits sind ja die behandelten Kanäle nicht prinzipiell gut oder gefährlich – es kommt immer auf den Kontext an. In dem Bewusstsein, dass man nicht alles verbieten kann, sondern eine gute Sicherheitsrichtlinie das Arbeiten der Kollegen unterstützt, statt es zu behindern, sind entsprechende Sicherheitsbasisfunktionen zur Verfügung zu stellen (vgl. Kasten).

Drucker als Leckagerisiko

Auch wo alle „klassischen" Ports und Schnittstellen geeignet gesichert sind, stellen Drucker häufig noch einen Leckagepunkt dar (s. a. [4]): Ausdrucke lassen 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. Und ohne fundierte Beweislage führt ein Vorfall schnell zu einem Generalverdacht für alle Personen mit Leserecht und bringt dadurch unnötigen Unfrieden in die Organisation.

Diese Sicherheitsherausforderung lässt sich weder mit einem allgemeinen Druckverbot für bestimmte unternehmenskritische Dokumente noch für einzelne Mitarbeiter 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 zu erfragen sind. Solche Informationen sollten dann auch auf dem Ausdruck 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.

DLP für Drucker

Sicherheitslösungen, welche 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 warum welches Dokument mit welchem Inhalt in welcher Stückzahl und über welchen Drucker ausgegeben hat – und auch Auflagen der Langzeitarchivierung werden gleich mit erfüllt.

Hier zeigt sich also ebenfalls der klassische Ablauf einer DLP-Architektur beim Export von Information:

_____ Druck aufhalten

_____ Information klassifizieren: Falls hierzu weitere Informationen notwendig sind, sollten diese vom Anwender in Form von Echtzeitdialogen erfragt werden. Hierdurch trägt man gleichzeitig zu einer besseren Security-Awareness bei, indem ein Benutzer auf die konkrete Gefahrenlage hingewiesen wird. Und so lässt sich trotz umfassenden Schutzes unternehmenskritischer Daten ein für den Anwender „verträglicher" Umgang mit kritischen Situationen erzielen. „Ganz nebenbei" erhält man zudem einen Nachweis der Compliance, da der Anwender beweisbar auf Risiken seines Handelns hingewiesen wurde.

_____ (bei Bedarf) Export-Information entsprechend der Unternehmens-Policy modifizieren: In einem konkreten von itWatch durchgeführten Projekt bestanden die Modifikation der gedruckten Daten bei Verschlusssachen mit der Einstufung „GEHEIM" beispielsweise aus der Ergänzung eines Titelblatts, das alle Information über Klassifikation, wer, wann, warum, an wen et cetera enthielt. Generell sind hier aber auch das Einfügen von Kopf- oder Fußzeilen, eines Wasserzeichens oder anderer Merkmale möglich – beim Ausdruck mehrerer Kopien kann dies auch das Aufbringen eines Identitätsmerkmals für jeden einzelnen Ausdruck umfassen.

_____ Archivieren: Das Archivieren kann natürlich in dem nativen Druckdatenstrom erfolgen. In der Konsequenz müsste der Betreiber aber alle Drucker, die je eingesetzt wurden, zur Beweissicherung bevorraten. Um diese kostenintensive Anforderung auszumerzen, wurde im angesprochenen Projekt ein druckerinvariantes Langzeit-Format eingefügt, welches die Lösung unabhängig von der verwendeten Infrastruktur macht.

Gelöscht oder versickert?

Daten müssen auch über ihren aktiven Lebenszyklus hinaus vor nicht-autorisiertem Zugriff geschützt werden, gegebenenfalls auch nach dem „Löschen". Betriebssystemeigene „Lösch"-Funktionen löschen bekanntermaßen nicht wirklich, sondern geben nur den belegten Speicher für die weitere Nutzung frei

DLP-Basisfunktionen

Überwachen der Leckagepunkte

Als Leckagepunkte kommen zunächst Kommunikations-Schnittstellen (inkl. Ports und Devices) infrage: Daher sind sowohl Datenträger (Filesysteme) als auch Netzwerkverbindungen, kommunizierende Ports (etwa Bluetooth, Modem etc.), aber auch Outputs mit Medienbruch wie Faxversand oder Ausdrucke zu überwachen. Darüber hinaus müssen Anwendungen im Fokus stehen, die fremde Inhalte laden und ausführen oder bestehende Inhalte weitergeben, hierzu gehören vorrangig Browser und E-Mail, aber auch Cloud-Services. Dabei sind proprietäre Protokolle hinreichend genau zu analysieren.

Prüfung der Daten in Echtzeit

Vor einem Daten-Austausch ist eine Inhaltsprüfung nach vordefinierbaren Kriterien erforderlich: Hierzu gehören Analysen anhand regulärer Ausdrucke, Labelling und beliebige, auch proprietäre Algorithmen als Plug-in, etwa im Bereich dynamischer Daten zur Sicherung von Ergebnissen bei Datenbank-Anfragen. In jedem Fall ist es von großer Wichtigkeit, dass der Handlungskontext verstanden wird und nachvollziehbar bleibt – das Zusammenspiel von Anwender, Netzverbindung, Rechner, Sensitivität der Daten, Quelle und Ziel ist daher in Echtzeit zu erfassen.

Auch ein pragmatisches Vorgehen „Frage den Anwender und speichere das Ergebnis als Label" ist dabei eine sehr gute Möglichkeit, um dem Handlungskontext gerecht zu werden. Denn meist kann gerade der Anwender die Kritikalität von Information sehr gut einschätzen und wird dabei auch nicht nachlässig verfahren, wenn er weiß, dass seine Klassifizierung langfristig, revisionssicher gespeichert wird und dadurch gegebenenfalls auch Haftungsfragen aufgeworfen werden, wo seine Einschätzung als Handlungsgrundlage für weitere Sicherheitsentscheidungen gilt.

Reaktionen auf den Kommunikationswunsch

Mögliche Reaktionen umfassen neben einem pauschalen Verbieten und Erlauben auch ein teilweises Erlauben (ggf. nach weiterer Analyse/Klassifizierung) sowie ein Kapseln: Analog zum „Sandbox"-Prinzip (wie etwa bei gekapselten oder „ferngesteuerten" Browsern) werden dann unbekannte Aktionen in einer kontrollierten Umgebung so ausgeführt, dass der Datenaustausch zu den produktiven Netzen detailliert überwacht wird (s. a. [1]). Im Übrigen sind die Aktionen (oder Teile davon) zu protokollieren und unter Berücksichtigung der Kritikalität der Protokolldaten gegebenenfalls verschlüsselt zu speichern. Beim Einsatz von Verschlüsselung ist im Hinblick auf die angestrebte Schutzwirkung (nur innerhalb des Unternehmens oder auch für vertrauenswürdige Dritte?) ein geeignetes Verfahren (bzw. Schlüsselparadigma) zu wählen.

– die eigentlichen Daten bleiben aber zunächst für jeden lesbar, der Zugriff auf den Datenträger erlangt.

Sensitive Dokumente – besonders auf mobilen Datenträgern – müssen jedoch so gelöscht werden, dass sie niemand wieder herstellen kann. Bei bestimmten Daten sind Unternehmen oder Behörden sogar gesetzlich dazu verpflichtet. Die Haftung für die Einhaltung dieser Gesetze liegt hier immer bei der Geschäftsführung respektive dem Vorstand und kann nicht an Dritte delegiert werden, auch wenn diese bestimmte Handlungen im Auftrag durchführen.

Neben den in Form des „Papierkorbs" einfach zu erkennenden Risiken auf NTFS-formatierten mobilen Datenträgern besteht das Risiko unzureichend gelöschter Daten aber auch auf weiteren, tieferliegenden Schichten. Besonders perfide sind Angriffe, die bestimmte interessante Informationen aktiv in Speicherbereiche verlagern, die sofort danach als „Bad Track" markiert werden, also als „schlechter" Speicher, auf den man mit Bordmitteln nicht mehr zugreifen kann.

Sicheres Löschen

Auch mit Datenträgern, die den gesamten zu speichernden Datenstrom verschlüsseln, löst man das generelle Problem nur teilweise: Denn der einfache und weit verbreitete Angriff mittels USB-Dumper oder erweiterten Werkzeugen bleibt hierbei wirksam [2,3].

Zudem wird gelegentlich übersehen, dass ein sicheres Löschen immer abhängig von der konkreten Bauart des Datenträgers ist (s. a. S. 62) und zudem in die Rechtestruktur eingebettet werden muss. Nicht zuletzt sind alle entstehenden temporären Dateien zu berücksichtigen. Dies alles sind Themenfelder, die man nicht dem Anwender überlassen kann.

Ein entsprechendes Sicherheitsprodukt muss daher auf der Basis vorhandener Berechtigungen und eventuell bestehender Berechtigungsdefizite beim Anwender automatisch temporäre Informationen und Metainformationen (z. B. Dateiattribute oder Ordnereinträge) identifizieren und passend zu den Eigenschaften des Datenträgers (Flash, magnetische oder optische Datenträger, Multiple Write oder WORM, …) den richtigen Algorithmus auswählen und anwenden, sodass zu schützende 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 transportiert man in dieser Nachricht dann auch gleich den Standort eines geeigneten Vernichtungsapparates oder einen Link auf den vorgesehenen Vernichtungsprozess.

Das sichere Formatieren vorhandener Datenträger (auch wiederbeschreibbarer optischer Medien) sollte ebenfalls gewährleistet sein. Und alle Verfahren sollten internationalen Standards und Auflagen beziehungsweise Empfehlungen des BSI folgen.

Fazit

Einem einzelnen Byte kann man nicht ansehen, ob es vertraulich, verschlüsselt oder öffentlich ist – und selbst wenn die Kritikalität einer Datei in Echtzeit erkennbar ist, benötigt man für eine korrekte Entscheidung noch die Information, in welchem Kontext gerade gehandelt wird. Die wirkliche Entscheidung in Sachen DLP muss immer situationsbedingt und eingebettet in einen komplexen Prozess erfolgen – Erfolge zum Schutz der Daten liegen daher nicht im bloßen „Etikettieren".

Eigenständige Netze oder Segmente schaffen in diesem Zusammenhang zusätzliche Sicherheit (vgl. [1]): Potenziell unsichere PCs lassen sich in ein virtuelles, eigenständiges Netz einschließen, um andere Teilnehmer nicht zu gefährden – ähnlich wie mit NAC-Lösungen für „Fremdrechner" im Haus, denen dennoch in begrenztem Maße Netzwerk, Internet und einige Fachinformationen zur Verfügung stehen sollen. Der Zugriff erfolgt dann zumeist über Standardverfahren (z. B. im Browser), Spezialanwendungen werden virtualisiert und über Remoteverbindungen dargestellt.

Wer seine Daten in solchen Netzen segmentiert und zudem wirklich alle Leckagepunkte und alle Stadien des Information-Lifecycle berücksichtigt, besitzt ein wahrhaft ganzheitliches DLP-Konzept und verhindert nachhaltig eine Gefährdung des Unternehmens-„Kapitals" in Form gespeicherten Wissens und gespeicherter Informationen. ■

Ramon Mörl ist Geschäftsführer der itWatch GmbH.

Literatur

[1] Ramon Mörl, Welches Tablet passt?, SecuMedia-Special Mobile Security, Juni 2012, S. 18

[2] Hilde von Waldenfels, Wie (un-) durchsichtig?!, Wie viel Transparenz Verschlüsselung braucht und erträgt, <kes> 2010#5, S. 6

[3] BSI, IT-Grundschutzkatalog, G 5.142 Verbreitung von Schadprogrammen über mobile Datenträger, www.bsi.bund.de/Content BSI/grundschutz/kataloge/g/g05/g05142.html

[4] Olaf Winkelmann, Rumgedruckse, Sicherheit beim Drucken – ein oft vernachlässigtes Thema, <kes> 2011#5, S. 10