GDD

GDD beteiligt sich an Konsultation zur Modernisierung der Europaratskonvention 108

Stichworte
Europarat
Europaratskonvention

Dieses Jahr feierte der Europarat den 30. Geburtstag des Übereinkommens zum Schutz der Menschen bei der automatisierten Verarbeitung personenbezogener Daten (Europaratskonvention 108), das von 43 Mitgliedstaaten ratifiziert worden ist und dem nach wie vor weitere Länder beitreten können. Das vom Komitee der Ministerbeauftragten des Europarates am 23. Mai 2001 angenommene Zusatzprotokoll ergänzt die Europaratskonvention um Bestimmungen über Kontrollstellen und zum grenzüberschreitenden Datenverkehr.

Im Rahmen einer gemeinsamen Veranstaltung des Europarats und der EU- Kommission anlässlich des 5. Datenschutztages am 28. Januar 2011 in Brüssel wurde eine Modernisierung der Europaratskonvention 108 initiiert. Nachfolgend hat der Europarat im Rahmen einer Konsultation Gelegenheit gegeben, sich zu den Modernisierungsplänen zu äußern.

Auch weil die EU-Kommission sich im Zusammenhang mit der Förderung universeller Datenschutzgrundsätze eine engere Zusammenarbeit auch mit dem Europarat vorgenommen hat – vergleiche Mitteilung der Kommission KOM(2010) 609 -, hat die GDD ihre Stellungnahmen zur Revision des EU-Rechtsrahmens für den Datenschutz auch in die aktuelle Konsultation des Europarates eingebracht.

Quellen
Informationen des Europarates über die Modernisierung der Konvention 108: www.coe.int/dataprotection
Stellungnahmen der GDD zur Revision des EU-Datenschutzrechts: http://ec.europa.eu/justice/news/consulting_public/0003/contributions/organisations_not_registered/gdd_de.pdf
http://ec.europa.eu/justice/news/consulting_public/0006/contributions/organisations/gdd_en.pdf

Tim Cappelmann, Langenhagen

DLP: Aufgaben zwischen Technik und Organisation

Stichworte
DLP
Datenpannen

Data Loss Prevention (DLP) soll den Abfluss wertvoller Daten aus Unternehmen und Behörden verhindern. Die Technik ist ausgereift, die IT-Organisation ist jedoch häufig noch nicht vorbereitet.

Data Loss Prevention, oft auch als „Data Loss Protection“, „Extrusion Prevention“ oder auch „Outbound Content Management“ bezeichnet, wird durch Marketingaktivitäten der Hersteller von IT Sicherheitslösungen verstärkt in den Fokus gerückt. Der Ansatz ist nach wie vor ungewohnt: Die Unternehmensinformationen soll nicht vor externen anonymen Bedrohungen geschützt werden, sondern vielmehr vor denen, die ganz legal mit Unternehmensdaten hantieren, den eigenen Mitarbeitern. Seit etwa drei Jahren ist das Problem des unerwünschten Datenabflusses aus Unternehmen oder Behörden wiederkehrend in der Presse. Call Center verlieren dort bearbeitete Kundendaten einer Krankenkasse, die britische Regierung verliert Datenträger mit sensiblen Daten ihrer Bürger auf dem Postweg, Kundendaten und Vertragsdetails eines deutschen Finanzdienstleisters werden der Presse zugespielt.

Doch wie ist dem unerwünschten und rechtswidrigen Datenabfluss beizukommen? In den genannten Beispielen hätte eine technische Lösung die Kommunikationsdesaster allein niemals verhindern können. Die handelnden Mitarbeiter durften gemäß der definierten IT-Berechtigungskonzepte durchaus entsprechende Abfragen ausführen und selbstverständlich auch Daten auf CD

Der Autor ist Security Consultant bei der AirITSystems.

brennen. Der Verstoß gegen etwaige Policies erfolgte – streng genommen – erst beim Verlassen des Unternehmens; zu diesem Zeitpunkt waren die EDV Arbeitsplätze bereits ausgeschaltet und die Daten in der Manteltasche. Der Datenverlust wird regelmäßig durch unachtsamen Umgang oder eben mutwilligen Datendiebstahl ausgelöst.

Der Einsatz von Data Loss Prevention-Technologien muss durch organisatorische Maßnahmen flankiert werden. Hier hapert es heute schon weit vor dem Einsatz von konkreten IT-Lösungen zur DLP.

Die Technik hingegen ist längst so weit: DLP-Produkte scannen Daten der zentralen Server auf sensible Inhalte, blockieren am PC die unverschlüsselte Kopie auf dem USB-Stick und verhindern beim Internetzugriff unerwünschten Datenabfluss via E-Mail, Internetupload oder den zunehmend beliebten Social Networks. Daten können heute in Bewegung genauso untersucht und reglementiert werden wie ruhende Daten auf Fileservern oder in Datenbanken. Leistungsfähige DLP Produkte kombinieren Agenten auf PC und Laptop mit Agenten auf den Servern und im Netzwerk und können so überall die Einhaltung der Unternehmenspolicy prüfen. Eine zentrale Administrationskonsole setzt das Regelwerk allumfänglich durch und ermöglicht im Gegensatz zu vielen technischen Einzellösungen einen wirtschaftlicheren Betrieb. Allen Produkten gemeinsam sind drei Optionen in der Durchsetzung der Policy. Daten können vom DLP Produkt automatisch verschlüsselt (1) werden, weiterhin ist das Blockieren (2) oder Erlauben (3) von Aktionen des Anwenders möglich. Mit diesen grundlegenden Aktionen lässt sich eine Unternehmenspolicy zu sensiblen Daten effizient aufbauen und durchsetzen. So dürfen sensible Daten das Unternehmen nicht unverschlüsselt verlassen, das gilt dank zentraler Administrationskonsole dann sowohl für USB-Ports als auch für E-Mail-Anhänge, CD-Brenner oder Internetkommunikation. Kundendaten dürfen ferner nicht auf beliebigen Druckern gedruckt werden, die Speicherung von schützenswerten Daten erfolgt nach DLP Regelwerk nur noch verschlüsselt und an zentralen, zuvor genau definierten Orten.

Die Produkte sind heute leistungsfähig und gut durchdacht: selbst Copy and Paste von sensiblen Daten in andere Dokumente oder Bildschirmfotos über die Microsoft-Zwischenablage tricksen die Technik heute nicht mehr aus. Das neu entstehende Dokument erbt dann automatisch die Vertraulichkeits-Klassifikation der Quell-Dokumente. Alle Agenten eines DLP-Produktes lernen voneinander und werden das neu entstandene Dokument exakt so behandeln wie die Policy es auch für die Inhalte des Originaldokumentes vorschreibt. Die Technologie des so genannten „Fingerprintings“ erkennt interne Inhalte von Dokumenten automatisch und heftet den Dokumenten Attribute zum weiteren Umgang an. Kombiniert mit bereits bestehendem Berechtigungsmanagement und möglicherweise vorhandenen Dokumentenmanagement-Systemen integriert sich eine DLP-Lösung nahtlos in den Lebenszyklus von Daten und Dateien. Die Produkte sind also längst vorhanden und ausreichend ausgereift.

Der Bedarf nach DLP Lösungen ist offensichtlich. Neben dem drohenden Reputationsverlust bei Datenverlust existieren seit der Novellierung 2009 auch reale Anforderungen aus dem Bundesdatenschutzgesetz (BDSG) . Wenn Unternehmen heute bestimmte personenbezogene Daten verlieren, ist dies im Zweifel der zuständigen Aufsichtsbehörde und auch den Betroffenen zu melden. Wenn die betroffenen Personen nicht direkt informiert werden können, müssen Unternehmen sogar die Öffentlichkeit über den Datenverlust informieren –mindestens in zwei bundesweit erscheinenden Tageszeitungen auf halbseitigen Anzeigen.

Woran hapert es in der Praxis?

Fazit an dieser Stelle. Der Bedarf an DLP ist unstrittig vorhanden und die Produkte sind marktreif. Wieso ist der Verbreitungsgrad der Lösungen dann heute noch so vernachlässigbar gering? Die Antwort: Das Ursprungsproblem ist in der Regel noch nicht ausreichend diskutiert und gelöst. Bei einer implementierten DLP-Lösung steht der IT-Fachmann vor einem sensiblen Thema, denn zwei Fragestellungen kann der Systembetreuer schlicht nicht selbst beantworten:

a) Welche Daten sind im Unternehmen schützenswert?
b) Welche Spielregeln sollen zukünftig im Umgang mit den Daten gelten?

Die Vorgaben dazu müssen von anderer Stelle kommen. Die IT-Abteilung bleibt hier in der Rolle der Exekutive, die legislative Rolle muss immer die Geschäftsführung einnehmen. Diese sollte das Controlling mit in das Projekt einbeziehen, Datenschutzbeauftragter und IT gehören ebenso an den Tisch wie Fachabteilungen und Arbeitnehmervertretung. Ein DLP-Projekt besteht aus technischen Maßnahmen (1), organisatorischen Festlegungen (2) und Anstrengungen der Unternehmenskommunikation (3), neudeutsch „Awareness-Maßnahmen“. Zur erfolgreichen Umsetzung brauch es ein interdisziplinäres Team. Längst eingeschliffene Handlungsmuster der EDV-Anwender werden geändert – das sorgt zwangsläufig für

Irritationen und auch für Widerstand. Ein DLP-Projekt lebt von guter interner Kommunikation und einer eindeutigen Legitimierung durch die Geschäftsführung. Es muss ein Projekt der obersten Unternehmensführung bleiben –und nicht ein weiteres Projekt „Sicherheit“ aus der IT-Abteilung.

Umsetzungshinweise

Die oben genannten zwei Fragestellungen (a/b) müssen individuell und im Kontext eines jeden Unternehmens beantwortet werden. Einige Hinweise bleiben jedoch allgemeingültig: Zur Frage, wo die schützenswerten Daten eigentlich liegen (Frage a), gehört zunächst die noch trivialere Fragestellung „Welche Daten sind schützenswert?“. Nach BDSG wären das zunächst personenbezogene Daten, aus Sicht des Unternehmens könnten das beispielsweise zusätzlich Vertragsdaten, Konstruktionszeichnungen oder Marketingpläne sein. Wenn ein Ziel zum DLP.Projekt und ein unternehmenseigener Schutzbedarf definiert wurde, ist der erste Schritt getan. Auf der Suche nach den Daten ist der gesamte Weg des IT-gestützten Geschäftsprozesses zu hinterfragen. Daten sollten immer einen definierten Weg innerhalb der Wertschöpfung zurücklegen. Datensätze entstehen zum Beispiel beim Zustandekommen eines Kundenkontaktes durch Handelsvertreter und werden viele Jahre nach Beendigung der Geschäftsbeziehung aus alten Backupbeständen wieder vernichtet.

Diese skizzierte Wunschvorstellung wird nach der Analyse des IST-Zustandes bei vielen Unternehmen schon verworfen. Oft geistern lokale Kopien auf Abteilungslaufwerken herum, Backups werden niemals gelöscht, Vertriebsmitarbeiter hantieren mit lokalen Kopien – teils aus Bequemlichkeit, oft jedoch auch für den miteinkalkulierten Fall, das Unternehmen irgendwann einmal zu verlassen und innerhalb der Branche die wertvollen Kontakte weiterhin zu nutzen.

Die zweite oben genannte Fragestellung (Frage b) nach zukünftigen „Spielregeln“ zum Umgang mit schützenswerten Daten ist da einfacher zu beantworten. Hier kann das Projektteam frei aufspielen und eine Policy am Schreibtisch erstellen. Wichtig dabei: Die Policy ist ein Werk der Unternehmensleitung und muss von dieser getragen werden. Das Projektteam arbeitet lediglich Vorschläge aus. Die oben genannten Grundbausteine „erlauben“, „verbieten“, „verschlüsseln“ können in einer Ablauforganisation sinnvoll, angelehnt an den Lebenszyklus der Daten, festgelegt werden. Hinzu kommt hier noch „informieren“, eine ergänzende Aktion, mit denen DLP-Lösungen auf spezielle Herausforderungen reagieren können. Immer wenn die DLP-Lösung Anwender in der Ausübung Ihrer Arbeit behindert, sollte das Produkt eine Alternative anbieten können. Installierte Agenten auf Laptops sollten kurze verständliche Informationen bieten, wie Anwender bei blockierten Aktionen nun trotzdem zum Ziel kommen. Wird der USB-Port gesperrt, weil der Anwender mit Kundendaten hantiert, muss der Anwender von der eingesetzten Software informiert werden. Gleichzeitig kann über kurze Hilfetexte der Policy-konforme Weg für die ausgeführte Aktion aufgezeigt werden. Ad-Hoc-Ausnahmen können durch schnelle Freigaben von Vorgesetzten legitimiert werden, kleine Hinweistexte können sogar elektronische Willenserklärungen enthalten – die den Haftungsdurchgriff nach KonTraG in die Geschäftsleitung verhindern. Die Benachrichtigungen können durch Agenten auf den PC oder über das interne Mailsystem zugestellt werden und erfolgen automatisiert ohne Eingriff des User Help Desks.

Chancen

Die erfolgreiche Implementation von DLP in die Ablauforganisation eines Unternehmens oder einer Verwaltung hängt von der Stärke des Managements ab, eine derartige Lösung zu etablieren. Datensicherheit erfordert es zwangsläufig, gewachsene und oft unkontrollierte Handlungsmuster aller EDV-Anwender zu kanalisieren. Prozesse müssen organisatorisch geändert und Geschäftsanweisungen formuliert werden. Die Technik kann eine ausreichend scharf formulierte Policy dann einfach durchsetzen – die Produkte sind ausreichend gereift. Oft ist aber die organisatorische Vorarbeit heute noch nicht geleistet. IT-Abteilungen denken immer noch in Produkten und nicht in Prozessen, Controlling und Geschäftsführung wagen es noch nicht, die Spezialisten in der IT zu hinterfragen.

Ein DLP-Projekt bietet die einmalige Chance, verworrene Infrastrukturen, Prozesse und Regelungen zum Umgang mit kritischen Daten neu aufzustellen. Begleitet von guter interner Kommunikation und Anstrengungen, die Geschäftsprozesse so gut wie möglich zu unterstützen, kann ein DLP-Projekt auch Sicherheitsbewusstsein schaffen und eine neue Sicherheitskultur im Unternehmen etablieren. Definierte Wege der sensiblen Daten unterstützen dabei enorm. Die einfache Anweisung „Personenbezogene Daten dürfen das Unternehmen nicht unverschlüsselt verlassen“ hilft hingegen nicht weiter. Unternehmen sollten das „Jahr des Informationsschutzes“ ausrufen und Ihre Mitarbeiter in das DLP-Boot holen. Wenn die Anwender den Grundgedanken mittragen, wird ein DLP-Projekt auch erfolgreich verlaufen.