HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

Török Szilárd
torok.szilard@gmail.com

GOVERNMENTAL LEVEL SOLUTION REGARDING DATA LEAK PROTECTION

Abstract

Information and data being kept by the users carry security risks in themselves due to rapid technological changes. In case of systems with larger networks it is worth examining what approaches and expectations need to be determined against data leakage.
The present publication therefore investigates the security application options of DLP networks from the point of view of the current challenges of cyber security.

A gyors technológiai változás miatt a felhasználóknál tartott információk és adatok önmagukban hordozzák a biztonsági kockázatokat. Nagyobb hálózattal bíró rendszerek esetén érdemes megvizsgálni, hogy milyen adatszivárgás elleni megközelítéseket és elvárásokat szükséges megfogalmazni.
Jelen tanulmány tehát a DLP-k hálózati oldalának biztonsági felhasználási lehetőségeit kutatja a kiberbiztonság aktuális kihívásainak mentén.

Keywords: *data leak prevention or data leak protection (DLP), endpoint protection, network DLP, Centralised Governmental IT System, National Info-Communication Service Provider ~ Adatszivárgást megelőző rendszer vagy Adatszivárgás elleni védelem, Végponti védelem, hálózati DLP, Központi Kormányzati Informatikai Rendszer, Nemzeti Infokommunikációs Szolgáltató Zrt.*

INTRODUCTION

The abbreviation DLP derives from Data Leak Protection or currently Data Loss Prevention. [1] The technological solution itself has a 15 year history. At first it was carried out only by disabling the different ports of the endpoints, later by controlling the incoming and outgoing data and files.

Around 2001-2002 in Hungary a solution was introduced that was developed by Hungarians, which was able to alarm or block based on certain behavioral patterns, then around 2004 it was suitable for more complex analysis such as: clipboard content control, print screen saving as evidence, separate management and regulation of user and desktop computers, the special control of applications and new policies based on collective functioning.

Around 2007 the monitoring, filtering solutions on network side turned up which were able to provide a solution for data leakage prevention during network functioning, along network protocols and according to different directions and content of the network.

The two types of – endpoint and network – DLP clearly pointed into one direction, namely a product that combines both functions.

The generally accepted definitions and their solutions were settled in the past few years, at the same time due to the multiple endpoint and network DLP solutions and the newer and newer special attacks and data leakage several approaches were developed.

Data leak protection however is far not a product, but the issue of real intention and resources on the client side. Even a good choice of solution can cause managing difficulties in the DLP system, eventually the time and energy invested in its introduction will not necessarily pay off.

Due to the related costs and the resource requirements of the process organization it can be clearly concluded that the selection and introduction of any DLP solution needs to be subject to a strategic decision and this is why DLP requirements expectations becomes necessary in government-wide planning.

The goal this publication therefore explore bases and security options of DLP solutions therefore to answer of the current challenges of cyber security.

General introduction of DLP

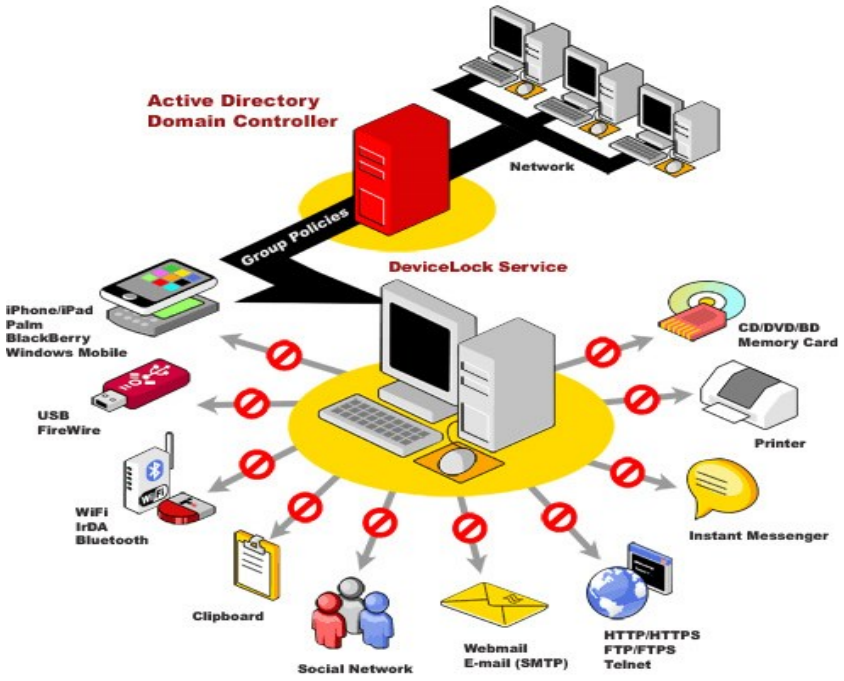
It has to be defined what general goals can be expected from a DLP solution:

- It is an efficient tool against internal threats
- It is a tool for enforcing IT security policies
- It supports the daily work of the security manager
- Built-in security concept, protection profiles
- Risk proportionate IT security can be developed
- Process based, minimum realistic approach
- Detects – incidence, frequency, alignment
- Reaction – approves, logs, disables, blocks, alarms.

A complex DLP solution includes central management, policy establishment, policy enforcement mechanisms that were developed specifically for this purpose.

The real users of the system often do not possess profound technological expertise (this cannot be expected), and are mainly from the fields of work process, data security, business management or law.

It is therefore necessary that the interface and policy generation of the system should be easily comprehendible and operable from a technical point of view even for laic users.



1. Figure. Device protection
http://biztonsagportal.hu/interju-kiterjesztett-adatszivargas-megelozes.html

The system is expected to be centrally manageable: separate interfaces are necessary to determine the data to be protected (eg. HASH), to develop the system of policies, to monitor the data flow, to intervene and to generate reports.

It is furthermore necessary to determine different user levels and authorizations.

2. Figure. The process of insider threat and its possible consequences source:
www.GTBTechnologies.com

Three DLP solution types, or approaches exist which will be described below.

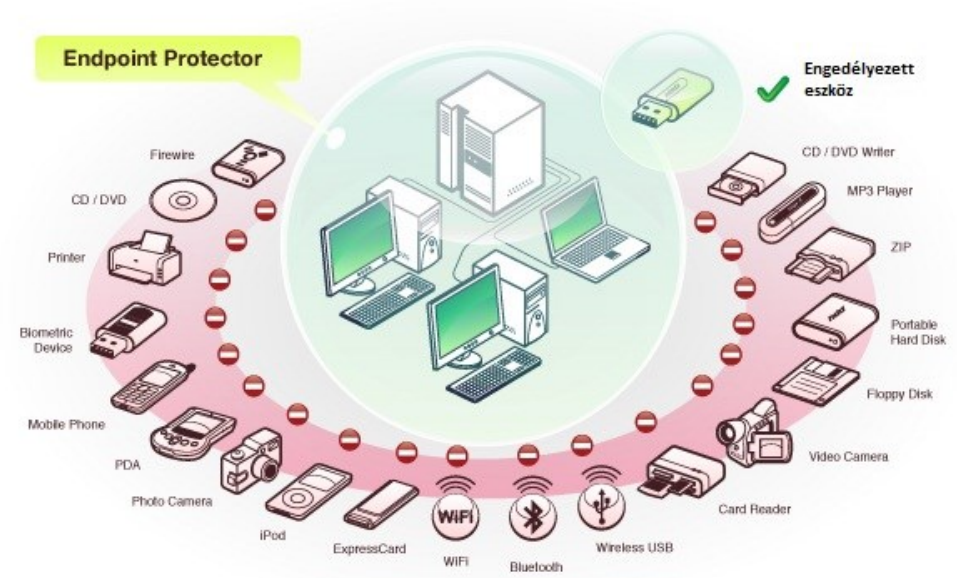
DLP approach: Endpoint DLP protection

The Port Protection approach provides solution almost exclusively for Windows clients, and typically tries to control the external communication channels, ports on desktops.

It derives from the approach itself that most of the solutions are not able to take the source of the data (eg. which directory or server) into consideration during data motion, moreover it does not include process/value generation based regulation.

The technical consequence of endpoint approach or DIU (Data In Use) [2] is that it can only operate with kernel driver level agents. This approach can cause system level clashes in case of compatibility and system updates.

Without proper developments and tests the client might face serious stability problems. An error like this may cause partial or complete Windows based client side breakdown, or it provides access with partial authorization. There were some unfortunate examples like the above in the case of Hungarian developed products, at the same time there was a significant improvement in stability.



3. Figure. Protection of endpoint
www.relnet.hu

DLP approach: Right Management

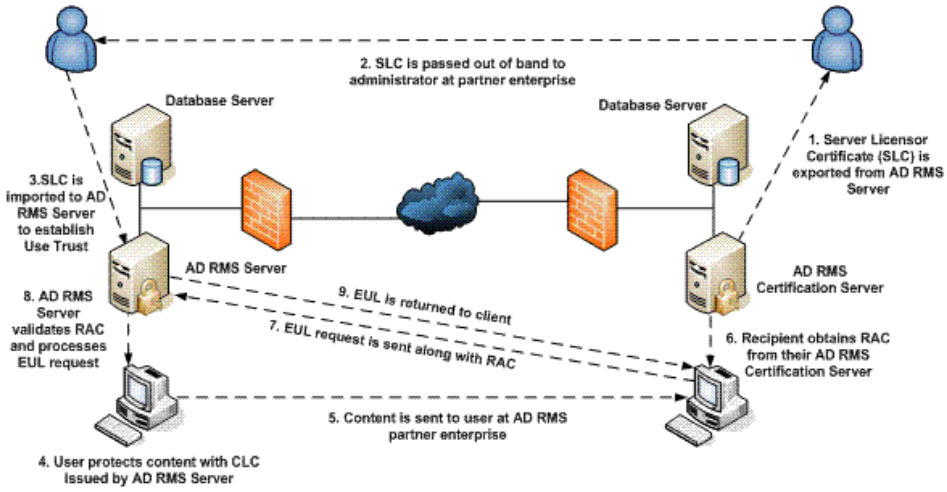
The basis of Microsoft RMS (Right Management Services) [3] is an open source encryption algorithm in which identification and/or encryption is implemented with the usage of two asymmetric keys.

The hindering of the leakage of confidential information is implemented by protection of the content and regulation of content usage. One of the possible leakage methods – among the first ones – is the intentional or unintentional forwarding of e-mails that can generate access to confidential data.

The goal of the RMS solution is not encryption, but the generation of a fingerprint that is typical of the original data. The simplest and most available RMS system is Microsoft RMS. Microsoft integrated this system into all of its current operations systems and its own Office product, and provides these products with the above system.

The RMS system is an XrML based Net web service which possesses a hierarchic and redundant architecture. It generates fingerprints with HASH algorithm.

The RMS clients work through API calls [4], the security calls are executed by a special DLL (Lockbox that manages the private key of the computer). Both, the computer and the user possess an internal certification.



4. Figure. RMS Trusted User Domain
http://technet.microsoft.com/en-us/library/dd983944%28v=ws.10%29.aspx

This RMS system is not compatible with other PKI solutions, not even with Microsoft's own PKI solution. Reason of this is that oddly their own asymmetric key system is operated to maintain dynamic operation. The utilised algorithms are similar to the PKI (RSA, AES), the certifications are in XML formats, and for the SSL web service an X.509v3 certification is necessary.

The vital attributes, advantages of RMS concerning data leak protection:

- Limited content access (Outside the RMS system it is not possible to read the document).
- Modification and printing can be limited
- Encrypted e-mail that can be only read by the recipients.
- The readability of the e-mail is limited in time.
- Control of Drag and Drop
- Copy/Paste blocking in case of copying from a protected document.
- Print Screen control
- It can be integrated with SharePoint, it automatically protects the content according to the user authorisations.

The disadvantages of the solution are worth mentioning – during the testing and usage of RMS the following deficiencies could be revealed:

- The optional templates are of limited availability: eg. maximum 20 templates are indicated, despite the fact that more templates have been defined in the system.
- Version control does not operate properly in case of MOSS 2007 integration
- Besides protected Office documents it is only possible to extend the range of RMS to (some) other types only with complementary (not Microsoft) products. In this case the risks concerning file filter drivers can increase, it is recommended to set up an independent file server with the activation of RMS extensions for the specifically protected documents.
- In some cases the clipboard operations are completely shut down when opening a protected document, which at the same time makes it impossible to use the copy/paste functions within the document.

DLP Approach: Content Filtering

The SANS Institute defines the DLP [5] in the following way: „Products that, based on central policies, identify, monitor, and protect data at rest, in motion, and in use, through deep content analysis."

Thorough content analysis, central policy system and the ability to manage the content on more platforms and locations have to be emphasized in the definition. If we choose this solution, the DLP system not only protects the sensitive data, but helps adjusting the policies and the technical policy system generated from them to the actual data flow.

Nowadays the primary goal of the introduction of a data leak prevention software is the detection, monitoring of data leakage in the web traffic and e-mail traffic of certain organisations and partners. In case of IT operation in public administration the recon of sensitive data on the central SharePoint server has to be emphasized.

Content recognition

According to the Content Filtering approach the task of the DLP solution is the precise recognition of content. Taking into consideration the fact that information flows in an unstructured way in many cases, the recognition of the context is of key importance (to whom, from who, when, in what form, with what other information) which not only increases the accuracy of recognition, but decreases the frequency of false alarms.

Moreover, the knowledge of numerous file formats is necessary in order to analyse the content. Analysis typically means fingerprint recognition, policy based recognition, document or document section recognition or statistical analysis.

Architecture

A good DLP solution is able to recognise the data at rest (on work stations and file servers), during motion (at any point in the network at gateways or near them) and during usage (copying, printing, e-mail sending), and is able to interfere in its usage if it is necessary.

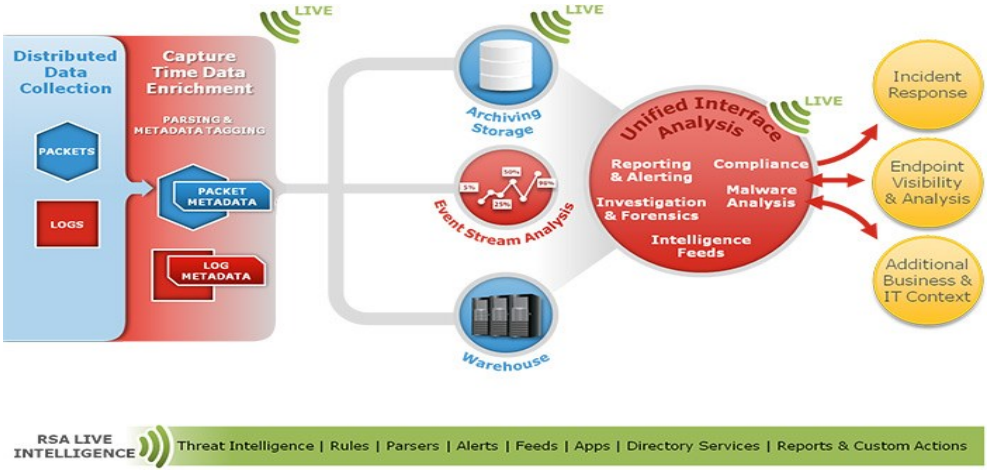
Regarding architecture the network DLP solution has a network sensor (in bridge or monitoring mode), gateway protection (e-mail and web-gateways, print-and file server modules can be accessed), and an endpoint application. Thus the protected information can be managed at any point. With the integration of PKI solutions of third party manufacturers the system is even able to recognise encrypted data contents.

Another vital ability lies in HASHING, namely in intense language analysis which is able to recognise confidential information in an intelligent way regardless of the language. For structured data formats (eg. credit-card number, bank account number, personal identification number, ID card number, etc.) separate definitions can be developed, furthermore these are mostly predefined in the system. The outstanding content recognition abilities are the core of these solutions which can operate equally on multiple levels of the IT infrastructure (network, gateways, end point).

Regarding data protection those data needs to be monitored that on the one hand can be defined with the help of keywords and regular expressions, on the other hand they are stored in highly protected systems.

In order to be able to monitor traffic towards the internet a sensor device needs to be set up. The sensor primarily analyses the communication on SMTP, HTTP protocol according to their data content, but the device is able recon and analyse data content in other protocols (eg. FTP, Telnet, POP3, IMAP, AIM, MSN).

As a matter of fact the sensor works like and IDS, therefore the traffic to be analysed needs to be monitored through one SPAN port of the central Switch.



5. Figure. RSA Data Loss Prevention Network
http://www.emc.com/security/rsa-security-analytics/images/chart-sa-marketecture-700px.jpg

With this solution it can be completely excluded that it would impact the procedure continuity due to malfunction of the device or due to a incorrect configuration. That traffic needs to be mirrored to the SPAN port, through which the outgoing (leaving the organisation) traffic of the appointed organisations can be monitored. Certain traffics can be distinguished by defining IP addresses and address ranges.

In order to be able to distinguish certain people and organisation units the DLP system can be implemented by connecting to a central address storage system. This way the monitoring policies can be directly assigned to people and organisational units.

In case of content monitoring policies data surveys need to be conducted at the involved organisations in order to be able to determine those data categories which will be monitored by the DLP system.

It is necessary to create a classification pattern or the default profile of the DLP system needs to be used.

As a result of policy system planning two types of sets of policies can be developed:

- Set of policies which determine what classification a file/document should be assigned. Based on these designations the user of the system can decide the relevance of certain incidents.
- Set of policies which determine the management of designated files, namely which user operations are allowed and which are not in the given data category (whether e-mail sending is allowed).

REVIEW OF CENTRAL GOVERMENTAL IT

The goal of the Digital Renewal Action Plan [6] 2010-2014 – as a tool of the national info-communication development strategy formulated in the New Széchenyi Plan [7] - is the utilisation of modern information and communication technology in order to ensure transparent, more secure, cheaper and more efficient operation of the state.

Central Governmental IT System

In accordance with the directives of the European Union and the central goal of the Hungarian Government to improve the efficiency of public administration, the implementation of a Centralised Governmental IT System (KKIR) was finished in October 2013. [8]

The project is the organic continuation of the Standardised (IT) Infrastructure Programme (EIP) launched in 2008 then suspended in May 2010. In the framework of EIP the integration

of IT systems, IT networks and applications used by the institutions has been launched in certain institutions of central public administration.

The primary goal of the KKIR project was to replace the non-branch specific IT elements operating in certain institutions by centralised services, thus unjustified parallel developments and unnecessary operational expenditures can be avoided. This way the advantages of basic and advanced level infrastructural and network data transfer services can be utilised by the employees in public administration.

The extremely important fundamental principle of an efficient and unified governmental IT is a central architecture that is able to serve the institutions in a centralised and standardised way.

The Government Decree of 1314/2010. (XII.27.) named the Centralised Governmental IT System Development project [9] as an accentuated project, and the National Info-communication Service Provider Ltd. (NISZ) was assigned with the implementation of the project.

The company as the operator of the governmental info-communication infrastructure primarily provides governmental IT solutions (through the National Telecommunication Core Network – NTG).

309/2011. (XII.23.) Government decree [10] the category of centralised IT and electronic communication services that are provided by NISZ, and defines the category of those organisations which are obliged or entitled to use these services.

The results of NISZ in central operation

In the framework of KKIR such a complex system was developed that makes it possible to operate a secure, high quality and cost efficient info-communication infrastructure and basic service in the central government.

By the end of the KKIR project the Standardised Infrastructure will provide services to the Ministries. The direct target group of the project will be the institutions of central government (abbreviations: NFM, EMMI, NGM, VM, KIM, BM and the Prime Minister's Office) the employees and associates of these institutions.

Throughout the project the central address storage was standardised (domain-consolidation), obsolete work stations (2640 pcs PC, 350 pcs notebook) were replaced by modern devices and theye were installed with a standard environment in order to be able to operate the newly introduced management systems efficiently operated by NISZ. [11]

Identical, modern platform was installed at the new desktop environment, and OPEN Doc Format (ODF) was set as default.

As a result of the new management systems now a standardised system supervision and software management operate within the Standardised Infrastructure. Within the framework of the project, group work applications were installed where remote access is provided as well. Regarding technical content a shift to Windows 2008R2, Exchange 2010, SQL Server 2008, SharePoint Server 2010 systems was implemented.

In the framework of KKIR project NISZ Ltd. developed a mutually substitutive (geo redundant) server environment – 46 pcs new server, 1 pcs new computer room, 2 pcs redundant storage, 2 pcs redundant devices for e-mail archiving were procured and put into operation. With these devices the availability time of the extended EI system can increase, and the quality of the service is improved with the operation and IT security solutions.

In order to modernise the network infrastructure the firewall system was improved, the institutional internal backbone networks were made redundant, and the external station connections were extended so that each station would operate with standardised, redundant network connection.

NISZ IT Security

The reorganisation of NISZ started in February 2012 with the appointment of the new CEO and reorganisation of the management which accelerated the reorganisation process. The management's mission was that NISZ would provide high quality, cost efficient and reliable electronic services to its users – public sphere, residents and businesses – which help their clients manage their everyday activity easier, faster, environmentally responsibly and securely.

In May 2012 an independent IT Security Directorate started to operate at NISZ Ltd. Its goal was to develop a standardised, transparent, controllable and homogeneous IT security system and policies in the field of IT security and regulation that operate according to effective laws, standards and professional recommendations.

In 2013 the staff of IT security directorate was significantly extended in accordance with new tasks and projects.

DLP IN GOVERNMENT

Selecting DLP type

The proper DLP solution needs to include the following type of solutions by SANS Institute [12]:

DIM (Data In Motion): The DLP network component should continuously monitor and track network traffics:

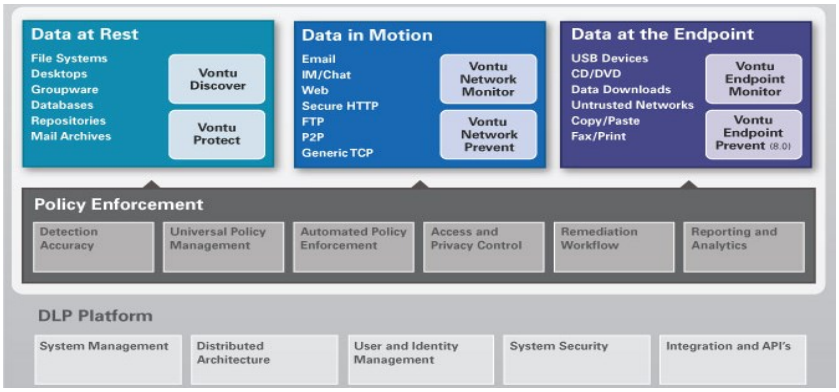
- Make sensitive information exiting the system measurable on a risk level.
- It should monitor and log (should be able to block) the unauthorised forwarding attempts of sensitive data in real time.

DAR (Data At Rest): It should protect the data stored on network resources (file servers, databases, etc.) from unauthorised actions.

- The system should be scalable
- It should reveal the sensitivity of the data available in file sharing, SAN/NAS systems, databases and other records.

DIU (Data In Use): The endpoint protection component should continuously monitor and track sensitive information stored in work stations and user activities, and prevent data leakage incidents:

- It should seek and protect sensitive information on desktops and mobile computers
- It should provide real time protection



6. Figure. DAR, DIM and DIU in Vontu solution
http://www.emagined.com/vontu_data_loss_prevention.php

Based on these types and taking the Centralised Governmental IT System into consideration basically the network DLP solution type can result in an efficient IT security solution.

The usage of network DLP in Governmental IT

The network DLP solution can be applied in the standardised IT system of the Government, and its advantage is that its usage does not require substantive user contribution, the operation of the system does not influence their activity.

The goal is to control data motion and hinder the exit of data from protected environment through communication channels.

It depends on the manufacturer how many communication channels the product is able to control, but the basic goal of the product is to control FTP, HTTP channels, e-mail and instant messaging channels and encrypted channels.

Cloud based communication might be integrated into the abilities of the systems, this is important because a cloud solution was developed on governmental level (Governmental Cloud, abbreviations: Gov-Cloud or KOF [13]).

Depending on the choice of solution the communication channels either need to be filtered natively or using an external supplier's product.

The internet traffic can be analysed with the usage of some kind of a proxy server, electronic mails are in many cases controlled through e-mail filtering applications. It is of great advantage if the DLP system can cooperate with as many products of external suppliers as possible.

Besides the control of communication towards the external world, the control of internal network traffic can be also the task of DLP.

Besides the usage of proxy servers the ability of monitoring the network is a useful and important attribute. Generally the systems can monitor (eg. on a Switch SPAN port) the traffic with some kind of a mirroring method, but other methods can be applied as well in case they do not weaken the performance of the system and the malfunction of the device does not jeopardise normal task management.

Internet network management

The traffic can be mirrored by the system or can be monitored other way. The normal management cannot be affected by monitoring, at the same time each port needs to be monitored.

Intervention/modification in traffic: the DLP solution monitors the traffic, and if necessary, it can intervene. This can take place natively (intervention in TCP session) or with a third party software (web proxy, e-mail filter).

The network component of the DLP system should be able to recon sensitive data transmitted through the network, to monitor traffic and block traffic:

- In case of monitoring the network the system should support the following protocols and systems: HTTP/HTTPS, FTP, SMTP, POP3, IMAP, AOL, IM, Google IM, MSN IM, Yahoo IM, Telnet.
- An incident should be generated if a policy breaching data transmission takes place.
- In case of blocking network actions the analysis of SMTP, HTTP, HTTPS, FTP, ActiveSync should be supported among network protocols. The system can execute the following actions with the data breaching the policy system: logging, blocking, in case of a policy breach on SMTP protocol in addition to the above quarantine and encryption can be executed.
- The system should support the monitoring of data traffic between e-mail boxes in internal e-mail systems (Microsoft Exchange).
- The system can execute the following actions with the data breaching the policy system: logging and blocking.

E-mail filter integration
Electronic mail is one of the most important channels, the filtering of this is of key significance.

It is expected that the DLP system can be integrated to a third party email filter application. It has to know Microsoft Exchange and Lotus Notes from the email sending systems minimally.

Proxy integration
Assuming a centralised internet exit, a web proxy server needs to run the complete internet traffic.

The task of web proxy applications is content filtering, thus they can analyse the incoming and outgoing packages which is expected.

It should be able to look into the SSL connection with the help of a proxy or with an own solution.

Internal network
DLP systems are typical installed concerning border protection, but the monitoring of internal network traffic might be expected.

Managing mobile devices: it should be able filter the traffic directed towards the mobile devices. Managing clouds: it should be able to filter the internal traffic directed to the Gov-Cloud.

Managing virtual devices: the simple cloning method of virtual devices pose multiple risks from a data leakage point of view, thus this problem should be tackled by the DLP system. As a result, complete functionality can be expected in case of virtual devices.

Endpoint protection in the Government

Endpoint usage: the components installed on the desktop and mobile work stations need to continuously monitor the end users' activity in real time, and if necessary it needs to be able to intervene as well.
The following general functional expectations can be formulated:

- Printing: The system does not allow the transfer of sensitive data to the printer.
- Clipboard management, print screen saving: In case of a file containing sensitive data, the disabling of print screen and clipboard restricts the potential channels of data leakage. If a sensitive document needs to be made available to a larger category, then this ability can be especially useful.
- Mobile devices: On mobile devices it is possible to take out great amount of data from the organisation in a short period of time, thus avoiding border protection. It is important to be able to control the physically connected mobile devices at each endpoint: USB key, mobile wreck, CD, DVD, etc.
- Disabling applications on using sensitive data: It should be limited through which application should be the file containing sensitive data accessed. The file level access management can be adjusted by proper authorisation management of the applications.

DLP answers to incidents

- Incidents can be reacted by several actions depending on the fact what is the level of the incident. The scale can range from reporting to deleting the file (or database) containing the sensitive data.
- Reporting: The incident will be recorded. The record can be retrieved if it is necessary or it can be included in a regular report. This is a detective control, it is not able to hinder the leakage of sensitive data.

- Explaining the incident: It requires an explanation from the user before any action that can jeopardise sensitive data. If the user cannot explain the action, the action will not be executed. This a detective control too, it is not able to hinder intentional data leakage. However, it is able to reduce unintentional data leakage.
- Quarantine: The file containing sensitive data needs to be placed in a quarantine. The file placed in quarantine can be only accessed by the authorised users. It is a preventive control, leakage of sensitive data can be hindered with it.
- Encryption: The system encrypts the object containing sensitive data. It is a usual function when sending an email. It is good for reducing unintentional data leakage, but it does not protect against hostile activities.
- Deletion: The object containing sensitive data is deleted. The usage of this function is not recommended, or just with very reasoned settings and control – given the fact that it can result in serious data loss.

Recon on data storages

In order to hinder data leakage it is important to know what kind of sensitive information is contained in the data assets of the organisation and where they are located. The mapping of this is important task of the DLP system.

The attribute of a professional DLP system is that it can manage several types of data storages and mapping does not cause problems in performance.

According to new data storage practices, it is important to be able to manage virtualised storages and data stored in Gov-Cloud.

As a result of the mapping, it can be seen where the data is located in the data asset that meets the predefined criteria, furthermore it can make a Hash from the database or file that are considered important. During future searches these hashes can be monitored in other databases, files or communication channels, thus hindering the leakage of these files or databases.

- Managing scanned files, databases: A report should be made based on a search according to the defined policies. It is useful if the system sends feedback about certain assigned files or databases. It is expected that the object containing sensitive data can be transferred to quarantine, can be encrypted or deleted.

SharePoint, Linux and Windows file servers, SAN and NAS

It should be able to map the data assets and search in it with the above described analysing techniques. Usage is significantly easier if only a certain part of the directories can be controlled.

In case of file server sharing the control of CIFS, NFS and WebDAV based sharing is expected, furthermore it should recognise and list encrypted files as well.

Oracle, MSSQL, IBM DB2 and other optional databases: Mapping data assets with the above described analysing techniques. The time and method of mapping can be configured.

- Fingerprinting: The system can efficiently generate fingerprints of great amount of data. The fingerprint generation should be configurable and schedulable.
- Pattern search: The sample search (fingerprints, regular expressions, dictionaries, etc.) on the devices under monitoring should be executed as efficient as possible.

The system should be able to do split search and scheduled search. The endpoints and servers should participate in the search through the installed Agents.

Managing user interfaces and users

The status of external components of the system should be easily accessed, if possible from one location. It should contain the version of the component, the date of the latest updates and information on what sample search it executes. The management of the components should be executed from the central interface.

Reports, alarms or status reports of components should be indicated on the home page in a customised way.

The system should be connectable to AD (Active Directory). The registration of new users and identification should be done through the AD. The system should be able to generate cues. These cues should be assigned to AD groups.

It is more advantageous if it can manage the given DLP system with the better known Identity Management systems.

Incident management

In case of breaching the policy system the solution needs to provide a review into the incidents (arranged into incidents), set a notification and provide manual remedy or request a notification about the solution.

The filtering and arranging aspects of the incidents should be able to process identification number, date, type (network, datacentre, endpoint) severity, status, validity, the person/group assigned to the incident, policy breaching user, protocol or action, breached policy and action taken by the policy.

Status and person/group need to be set as search terms in a given time interval, furthermore it has to provide filtering terms for the search or exception management and the search itself could be saved (in a modifiable way).

The system automatically assigns the following to the incidents:

- identification (assigning to person or group)
- details of the incident (who committed a breach in the policy, when, with what, and what kind of policy).
- what was the reaction of the system
- severity level
- validity setting
- investigation (to whom the incident can escalate) of responsible (person or group)
- investigation of deadline
- status
- possibility to comment
- sending email notifications

All the aspects can be searched among the incidents, and besides a search can be executed according to the organisation of the perpetrator and deadlines.

Certain phases of investigation of incidents can be commented. The status of the investigations can be followed by the authorised staff. The incidents should be exportable into generally used formats.

Reporting possibilities

The system should have its own built-in report compilations. These on the one hand help prepare for audits (eg. PCI DSS), on the other hand they serve as a sample for preparing own reports.

The reports should be embraceable and comprehensible for those who come from the field of business.

The system should make it possible to generate summary reports according to the following aspects:

- according to organisation
- according to incident type
- according to breached policy
- according to data definition
- according to severity
- according to status
- fulfilment/compliance summary

The system should be able to generate trend indicator reports according to the following aspects:

- according to organisation
- according to device type
- according to incident type
- according to breached policy
- according to severity
- incident remedy trend indicator

Data center component

The data centre component of the DLP system should be able to recon the sensitive data in the systems below:

- File server sharing
- Database servers
- Data storages

In case of file server sharing the analysis of CIFS, NFS and WebDAV based sharing can be expected.

Based on the policy system the following actions are indispensable regarding the files: logging, deletion, modification of file authorisation, moving to dedicated directory, quarantine, authorisation, execution of automated counter actions (based on policies).

Throughout the analysis of database servers Oracle, Microsoft SQL and IBM DB2 database management systems are supported.

Throughout the analysis of data storages Microsoft SharePoint, Microsoft SharePoint Online (Office 365), Lotus Domino and Microsoft Exchange Server should be supported.

SUMMARY

In order to prevent governmental level data leakages, basically the introduction of a network type DLP solution is recommended in the centralised governmental IT system.

Based on the review of DLP solutions, my previous publications about governmental cyber-attacks [14][15][16][17], and analysis of possible requirements the following most important requirements can be formulated:

- Filtering network traffic
- Analysis of file sharing on network storage
- Control of endpoint activity
- Indexing of file or database content, recognising coherent data
- Recognition of encrypted files

- Recognition regular expression based data
- Management of previously built-in policies based on international standards
- Integration of Active Directory
- Preservation of original files, emails as proof in case of alarms
- Management of built-in alarm and incident management work processes
- Automatic severity classification of alarms
- Supporting analysis of alarm, comprehensive report generation and filtering
- Adjusting to logging and analysis systems

In case of a governmental level introduction the DLP solution might need to be extended with a system managing mobile devices (Mobile Device Management – MDM).

It has to closely cooperate with the logging and analysis systems of NISZ and with the operated specific systems, furthermore a customised access needs to be developed for the Governmental Incident Management Centre (Gov-CERT) to implement special queries and searches.

References

[1] *Data Loss Prevention* in Wikipedia (12 march 2014), The Free Encyclopedia, downloaded: 5 May 2014, source: http://hu.wikipedia.org/w/index.php?title=Data_Loss_Prevention&oldid=13290439

[2] *Data In Use* in Wikipedia (12 march 2014), The Free Encyclopedia, downloaded: 5 May 2014, source: http://en.wikipedia.org/w/index.php?title=Data_in_Use&oldid=599357970

[3] *What is Microsoft Dynamics Retail Management System (RMS)?* Microsoft, downloaded: 5 May 2014, source: http://www.microsoft.com/dynamics/dynamicsrms/retail-management-system.aspx?pageID=1

[4] *Application Programing Interface* in Wikipedia (10 Jun 2014), The Free Encyclopedia, downloaded: 11 Jun 2014, source: http://en.wikipedia.org/w/index.php?title=Application_programming_interface&oldid=612421786

[5] *Understanding and Selecting a Data Loss Prevention Solution,* SANS Institute, 2007, downloaded: 12 May 2014, source: https://securosis.com/assets/library/reports/DLP-Whitepaper.pdf

[6] *Digital Renewal Action,* Hungarian Government, 2011, downloaded: 12 May 2014, source: www.nih.gov.hu/download.php?docID=24683

[7] *New Széchenyi Plan,* Hungarian Government, 2011, downloaded: 12 May 2014, source: http://palyazat.gov.hu/uj_szechenyi_terv1

[8] *Realize of Modernized the Centralised Governmental IT System (KKIR),* Hungarian Government, 2011, downloaded: 12 May 2014, source: http://www.nisz.hu/node/110

[9] 1314/2010. (VII.27.) Government decree about Centralized Governmental IT System Development Project

[10] 309/2011. (XII. 23.) Government decree about services of the Centralized Information Technology and electronic newscasts

[11] *Close up EKOP KKIR project at National Info-communication Service Provider,* NISZ Ltd., 12 Dec 2013, downloaded: 12 May 2014, source: http://www.nisz.hu/node/209

[12] *Data Loss Prevention,* SANS Institute, 2007, downloaded: 12 May 2014, source: https://securosis.com/assets/library/reports/DLP-Whitepaper.pdf

[13] Governmental Cloud System, Hungarian Government, source: http://kof.hu/informaciok

[14] Török Szilárd: „Some Aspects of cyber attacks in 2011", Hadmérnök, VI. Évfolyam 2. szám; http://www.hadmernok.hu/2011_2_torok.pdf

[15] Török Szilárd: „Hungarian experiences in the light of cyber attacks in 2011", Hadmérnök, VII. Évfolyam 2. szám; http://hadmernok.hu/2012_2_torok.pdf

[16] Török Szilárd: „Anonymous in the World and Hungary", Felderítő Szemle, 2013. XVII. 3-4. ISSN 1417-7293, page 228-243.

[17] Török Szilárd: „Hungary's cyber defense readiness from the perspective of international recommendations", Hadmérnök, IX. Évfolyam 1. szám; http://hadmernok.hu/141_20_krasznaycs.pdf