EUROPEAN DATA
PROTECTION SUPERVISOR

Inspection of the OLAF IT security infrastructure

Report

Introduction

Following the adoption of a dedicated Information Security Policy and a secure implementation plan, OLAF has developed several complex and large scale IT infrastructures in order to support its investigation activities and guarantee its operational independence. These tools (IT applications and systems such as the Electronic Document Management System), which were initially hosted by the Data-centre of the European Commission, are now transferred to the OLAF premise and will be managed directly by OLAF staff.

The EDPS has received numerous notifications from OLAF dealing with data processing activities which run on the same IT infrastructure. In order to ensure a consistent approach to OLAF' security measures, the EDPS has decided to analyse them in a horizontal way, rather than doing it in the context of each particular prior checking notification. Conducting this analysis with a dedicated security inspection also contributes to a better handling of the confidentiality dimension of these security measures. Additional assessments on targeted security issues might be added to each prior check in order to complete the analysis of the specific security elements of the application they are describing.

The EDPS has decided that the scope of the inspection is limited to the following IT infrastructures which are hosted into OLAF' premises:

- Core Business Information Systems (CBIS) which are the information systems dealing with OLAF operational information,
- Secure External Gateway Services (SEGS), the systems which provide a secure exchange of information with OLAF partners,
- Anti-Fraud Information Systems (AFIS), systems provided to Member States and to third countries in the field of mutual administrative assistance in Customs and agriculture matters,
- OLAF specific physical access control.

The inspection did not cover other IT applications used by OLAF and managed by the Data-centre of the Commission. Within this framework, the EDPS inspection applied to OLAF infrastructure, personnel, organisation and technologies.

I. Facts and evaluation

The main objective for the inspection was to gather facts on the implemented or forthcoming security and data protection measures and compare them with the requirements in that field in order to assess their compliance with legal (Article 21, 22 and 23 of Regulation (EC) No. 45/2001) and technical (ISO 17799 and ISO 15408) standards.

The inspection report is built on the following actions undertaken by the EDPS in the course of this inspection:

- a visit of the OLAF premise where the IT systems and application are hosted
- a meeting with the OLAF Local Information Security officer (LISO) and the Data Protection Officer (DPO),
- a questionnaire focused on salient points of OLAF security elements and policy.
- the analysis of documents related to the security policy provided by OLAF

The EDPS is aware that some systems and procedures presented during the visit are still in a development phase or are even only planned at this stage. This point has been taken into account in the analysis of the provided answers and this final report.

The efficiency of the implementation of these security measures will be assessed next year by an in-depth security audit foreseen by OLAF, to which the EDPS will be associated as an observer.

A. Risks and incidents management

In 2002, the Court of Auditors conducted an IT network security audit of the Commission. It selected several DGs, including OLAF, for an in-depth analysis. It concluded that OLAF' IT systems and applications should be supported by a dedicated network (independent from the one provided by the Commission). Following this recommendation, OLAF commissioned two studies, in 2004 with Telindus and one in 2005 with Trasys, in order to quantify the risks, to evaluate the vulnerabilities of its activities and to validate or enhance security measures.

The quantitative model used in the first study was ROSI (Return On Security Investment), which provides a security benchmarking tool for planning security strategy. It was completed by an analysis of the compliance of the security controls with ISF's (Information Security Forum) "Standard for Good Practice for Information Security". The second security study was based on Octave (Operationally Critical Threat & Vulnerability Evaluation) which examines organizational and technology issues and defines the information security needs of the organisation. These studies targeted the integrity and confidentiality issues of information processed by the main OLAF information systems, the CBIS.

Delivering recommendations on the most appropriate network architecture given OLAF needs and the risks evaluated as well as recommendations on the global security architecture for CBIS, the studies provided the main lines of the call for tenders initiated in 2005 by OLAF for the procurement of IT and physical security

systems. Following the end of the development phase, an in-depth security audit is planned for next year.

Among the security measures implemented, OLAF is building a Security Information and Events Management system (SIEM). This system will keep a record of logical and physical security-relevant information and events. It will analyse them, detect and report deviations from established policies.

A classification of security incidents/events (minor, important, critical, etc) which could occur and the management (handling procedure) of each type of them will be defined and implemented by the end of 2007.

The SIEM will be managed by the Network Operations & Security (NOS) sector. NOS is made up of 4 EC officials. One of them has primary responsibility for smooth operations (including preventive maintenance) of the system. The other members of the sector are operational backup and are trained for daily operations of the system.

Key security management responsibilities have been assigned to different sectors (Human Resources, IT Production, Network Operations and Security, Application Support) according to a Duty Segregation Plan. These responsibilities are therefore distributed among the sectors without any possibility of sharing them. Outsourcing is allowed in some of these sectors but always under the supervision of an official and in compliance with Commission Decision (2006/548/EC, Euratom) of 2 August 2006 amending Decision 2001/844/EC, ECSC, Euratom.

Evaluation: OLAF has defined an ambitious and sound security strategy which was necessary, considering the sensitivity of its activities and the critical need for thorough management of the confidentiality and integrity of production data.

B. Documentation on security

OLAF organisational security policies are described in the 2005 OLAF Manual. A new version of the manual is expected at the end of the development phase of the new security infrastructure (2008). The OLAF Manual is available to all OLAF staff, both electronically (on the OLAF intranet) and in paper form.

Staff are informed about the organisational security policy through the following channels:

- The OLAF Manual;
- Security Training dispatched monthly to newcomers;
- Mandatory training on EUCI (Classified Information of the EU) by DG ADMIN DS at completion of the staff vetting procedure;
- ad-hoc CBIS training sessions will be scheduled when deploying the new secure desktops / security badges to end-users;
- Security pages on the OLAF Intranet.

The documents supporting the organisational security policy are produced and maintained up-to-date by the following officials:

- The Security Officer (LSO+LISO);

- The Data Protection Officer;
- The Documents Management Officer;
- Management responsible for security.

Briefly defined in the Duty Segregation Plan, the responsibilities of human resources, security and IT support staff will be detailed in the OLAF specific IT security Policy in the course of 2008.

The interoperability of OLAF specific security systems with those of the Commission are being defined and agreed in cooperation with the EC Security Directorate, ADMIN/DS. The agreement for the cooperation between the two services has been defined in a Memorandum of Understanding signed in 2007. The agreement defines the respective responsibilities of OLAF and of the Directorate Security in the management and supervision of access to OLAF using OLAF-specific security systems (physical access control, video surveillance, and intrusion detection).

Evaluation:
Considering the level of development of OLAF new security infrastructure, the EDPS considers that its organisational security policy is well-documented. Staff can easily have access to this policy through different channels.

C. Physical access control

OLAF also applies the strategy of independent management with respect to physical access control. Presented in the MoU between OLAF and the Security Directorate of the Commission (ADMIN/DS), OLAF has defined four different Zones (A to D) within the OLAF secure premises (the parts of the EC building J30 exclusively occupied by OLAF) and which are under its security responsibility.

Zone A represents the areas located beyond the security protections establishing the OLAF security perimeter and does not require additional security measures.

The staff offices are referred as Zone B. The management of office keys is a joint responsibility of the OLAF LSO, ADMIN/DS, and the OIB, according to procedures defined and controlled by ADMIN/DS. Office doors have to be locked when this area is unattended.

Zone C is defined as sensitive area, such as those hosting IT network and system equipment (computer rooms). Only authorised staff members have access to Zone C. An exhaustive list of persons with a permanent access right to Zone C is maintained by the OLAF LISO. 21 persons currently have permanent access right to the CBIS computer room, 22 to the AFIS computer room and 25 to the general-purpose computer room. The list is updated when required and communicated to ADMIN/DS.

Zone D, like Zone C, is considered a critical area. They represent rooms where OLAF operational information is directly accessible, i.e the Document Management Centre where the case files are stored. An EU Classified Information security area is under development within Zone D. Access to Zone D will require a fingerprint authentication for the identity check process. Outside working hours (07h00-20h00),

the entire OLAF secure premise will become a Zone D. The glass door barring access to OLAF lifts and access via staircases to enter OLAF will require D-type access control points. Only staff members with a need to access the OLAF secure premises outside normal hours are concerned by this policy. In compliance with the terms of the MoU, the EC Security Permanency will be provided with the means remotely to open the glass door in order to manage exceptions, like technical or safety emergencies.

Three fingers (template) will be enrolled. During the authentication process, the user will choose one of these three fingers. The possibility to use any one of the three fingers will reduce the risk of rejection due to injuries. The templates are only stored in the users access card. Fallback procedures managing failure to enrol or false rejection are not yet defined. OLAF has sent recently a notification of this biometric process for a prior check to the EDPS (registered as case 2007-0635).

The Central Access Management System which aims at monitoring the Zones previously defined is still under development. Its logs management policy will be established at the end of the development phase and submitted for prior-checking.

Since 2005, security clearance is requested for all OLAF staff, and the required level is EU SECRET. Until now 40% of the staff has been vetted. For interim and short term contractual staff, this security measure is not requested.

Apart from OLAF officials, three other categories of staff need to intervene routinely in Zone C:

- Office Infrastructures Bruxelles (OIB) staff and their related contractors (Dalkia, Kone, Simac, Pedus) intervene in this zone for cleaning services, building technical maintenance and refurbishment;
- DG DIGIT contractors (Intrasoft, Belgacom, Serco, Fujitsu-Siemens) who are in charge of the EC network and telephone equipment;
- ADMIN/DS inspectors and security guards.

A restricted list of authorised OIB and DIGIT staff or their related contractors has been defined in order to grant them access to the Zone during normal office hours. Vetting procedure is not required for this staff. This list is transmitted to ADMIN/DS and the security guards. Access outside normal office hours requires prior authorisation by OLAF and a report of the intervention is sent by ADMIN/DS who is supervising the intervention. All accesses are consigned in a logbook by the security guards at the entrance of the building. Access by personnel which are not on the restricted list requires prior authorisation by OLAF.

A restricted list for granting routine access is also established for OLAF contractors (Unisys, Getronics, Siemens). These support contracts require the provision of vetted personnel for IT systems management tasks. This is controlled by the contractors's security department and the clearance is communicated to the OLAF contract manager. Security clearance is not requested for interim or short-term contractual staff of OLAF.

Other OLAF visitors are registered and escorted by OLAF staff during their visit.

All paper versions of documents related to business data are stored in the Greffe. Procedures for accessing documents stored in the Greffe are defined in the OLAF manual. The Greffe acts as the EUCI (European Union Classified Information) registry of OLAF. Regarding the security measures, the Greffe is defined and managed as a Zone D. OLAF is implementing a clean desk policy for all the offices of the OLAF zone.

Evaluation:
OLAF is deploying a rigorous and reasonable physical security policy within its premise. The definition of four zones facilitates the security management of areas visited by numerous different actors.

The EDPS welcomes the application of the fingerprints measures only to OLAF staff who will clearly need an access to the OLAF zone outside the working hours or/and an access to IT applications which require such authentication process.

Requesting security clearance for all the staff and at such a high level (EU SECRET) is against the proportionality principle regarding data protection as well as security for which it could be even counterproductive. This process requests the collection of a lot of personal data which can only be justified if there is a clear need. This need has not been demonstrated. This vetting policy is also against the logic of a "need to know policy" which is an element of the OLAF security policy. The recruitment of staff has been subject to a notification for a prior check to the EDPS (case 2007- 006).

The EDPS welcomes that security clearance for interim and short term contractual staff of OLAF is not requested as this staff turnover is too high and National Authorities would not be able to clear them before the end of their contract. However the EDPS regrets that a dedicated security policy for these staff categories which would balance the lack of security clearance is not documented.

D. Logical access control

The Network Operations & Security (NOS) sector and the OLAF deputy-LSO have access to all the logs generated by access controllers to the CBIS and AFIS systems. They perform daily analysis of the firewall logs. These logs are not encrypted. Their management (storage, access, deletion, etc.) will be detailed in a dedicated policy. The future CBIS SIEMS will allow centralisation of security-related events generated by CBIS systems or applications. It will allow automatic analysis and reporting of deviances vis-à-vis established policies.

CBIS and AFIS systems clocks are synchronised by means of three network time servers as NTP protocol over UDP is not allowed through the CBIS firewall. Each has a built-in DCF77 receiver (Frankfurt atomic clock), with an antenna located in the upper floors of the building.

Following the duty segregation plan, application logs are only accessible by the managers in charge of respective applications, OLAF CBIS developers, application support teams and end-users (in the latter case the access is restricted to the logs they have generated). Oracle DBA's, which are vetted contractors, have also access to the

DB logs. Access may also be provided to ADMIN/DS or to OLAF investigators upon request from Management as part of security incident management and follow-up. Today the logs are neither encrypted nor centralised. They are stored on the application that generated them. The CBIS SIEMS will centralise these logs which will be accessible to and managed by NOS staff members.

The management of access rights respects as well the duties segregation plan. A request for access is sent by the business area in charge and registered/processed by the OLAF Helpdesk. Unit D8 (Information services) then creates systems/applications accounts required for the users.

For the CBIS, these access rights are linked with the creation of an USERID. This procedure will be performed by unit D5, which is in charge of managing Human Resources. The overall procedure which is based on elements still under development will be documented by the end of 2007.

The AFIS ISO (Information Support Office) keeps a record of all requests for access to the system. The ISO opens a call to the AFIS IT HELP DESK, which records this in its service management tool. NOS sector manages the AFIS security gateways, where all OLAF users are defined (around 150 users). Local CCN national authorities manage AFIS users using national procedures.

A strong password policy for AFIS users is defined and documented. However, the AFIS system does not enforce this policy.

CBIS will not request an end-user password policy as end-user system authentication is based on digital certificates and biometrics.

Some system administration tasks require using local system administrator accounts. Passwords for those accounts are subject to a strong password policy defined by the general Commission security policy.

Evaluation:
The EDPS welcomes the Duties segregation plan adopted by OLAF which corresponds to recognised international best security practices.

The EDPS welcomes the forthcoming release of the AFIS new generation which will enforce the already established strong password policy.

E. Security of communication and business data

The inventory of OLAF network connections and communications equipments is documented and available to Member States Administration Project Leaders and persons in charge of implementing telecommunication links with OLAF. This "Network guide" will be updated by the end of 2007 in coordination with ADMIN/DS as agreed in the MoU.

The use of mobile devices will be forbidden in the OLAF EUCI security area which is still under construction. A policy on the use of mobile devices in Zone C and D will apply.

A data encryption policy comprising PKI facilities is still under development, the management of this policy will be entrusted to the sector NOS.

The OLAF strategy for secure external communications is still under development. However, OLAF already defined two intermediate security classes between the EU public and EU Restreint ones established by Euratom regulation N°3 of 31/07/1958. Documents marked as "OLAF Operations" are handled in accordance with instructions in order to raise awareness of the receiver on the security obligations triggered by such documents. Information marked "OLAF operations -Special handling" requires that the receiver reads and also signs the handling instructions before having access to the information acting as a Non Disclosure Agreement.

Exchange of business information between external parties like the corporate IT system of the Commission and CBIS will be managed through a dedicated bridge located in the OLAF DMZ: the Secure External Gateway Services (SEGS). The SEGS should be operational in 2008.

The AFIS and SECEM ONE are the main tools used until now by OLAF to secure its communications with external partner. Communication of EUCI above RESTREINT UE will be secured in the future by using the New Cipher Network of DG RELEX.

In order to facilitate the collection of information to use in the fight against fraud, corruption and other illegal activities, OLAF has put at the public's disposal a Free Phone Service and a Fraud Notification System (FNS), a web based information system. Although the FNS has been directly implemented on the CBIS, OLAF has only recently undertaken the migration of the FPS to the CBIS. Both applications have been subject to a notification for a prior check to the EDPS[1].

Evaluation:
The EDPS welcomes the OLAF security handling instructions included in all its communications. However, the EDPS regrets that the two handling procedures sent together with OLAF marked documents do not contain a reference to data protection obligations.

The EDPS welcomes the migration of the Free Phone System undertaken by OLAF to the established independent infrastructure (CBIS) which will provide an enhanced anonymity expected by users of this facility.

F. Information security education and training
Security training on main IT applications and protection measures is part of the training package delivered to each OLAF newcomer. Following the introduction in 2005 of the new OLAF Manual, an updated security training was provided to each OLAF staff member. At the end of the development phase of CBIS and the new physical security measures, a new complete security training will be also given. Training on data protection for all staff is also planned in 2008.

---

1 FPS: case 2007-0074, FNS: case 2007-0481.

Officials of the Network and Operation Security sector as vetted EC official were trained on EUCI. They are regularly attending training on security of IT networks and systems, hackers' techniques, and incident handling. This training is provided by OLAF, EC security officials, and external training providers. The members of the NOS sector follow the security courses provided to EC LISO.

Evaluation:
Although not yet documented, the EDPS finds the OLAF practices for its security training policy as satisfactory and consistent with its needs.

II Recommendations

The following EDPS recommendations result from the evaluation of the fact-finding step carried out by the EDPS staff. They aim at providing guidance and elements for the necessary improvement of the systems.

- The interfaces between OLAF and DG ADMIN DS respective security responsibilities (these responsibilities have been defined in a MoU) need to be clarified in a document which will list these interfaces, how they are organised, who are involved in their implementations, etc.
- The vetting policy needs to be reviewed in order to be more focused on only staff who will really need this security clearance and not all OLAF staff. The need to know principle will be therefore better implemented and useless collection of personal data will be avoided.
- A dedicated security policy for interim and short term contractual staff needs to be developed and documented as these staff categories are rightly not subject to security clearance obligation.
- A reference to data protection obligations needs to be introduced in the security handling instructions accompanying OLAF communications.

III Conclusions

The EDPS is generally speaking very satisfied with the security measures implemented by OLAF on the IT systems and applications under its responsibility. He welcomes the fact that OLAF has adopted a new security infrastructure (CBIS) which is better adapted to the challenges raised by its missions. The launching of various security improvements will offer stronger data protection mechanisms. It is indeed of the utmost importance to fully ensure a high level of security of its systems, as well as to maintain its high level of performance.

Done at Brussels, 11 December 2007

Joaquín BAYO DELGADO
Assistant European Data Protection Supervisor