Vulnerability Assessment on Networked Systems of AAA Bank

(summary in english)

Milan, 12 January 2007

Hacking Team S.r.l.	http://www.hackingteam.it
Via della Moscova, 13 *20121 MILANO (MI) - Italy*	info@hackingteam.it
Tel. +39.02.29060603	*Fax +39.02.63118946*

Results

At the end of the ethical hacking activities carried out on systems and networks of AAA Bank Hacking Team deems the security level of the aforementioned systems and networks is adeguate while being thought of in conjunction with the kind of information handled and the type of business practiced.

According to the ethical haking evaluation performed from a physical point located outside the AAA Bank Network the security of AAA Bank systems and networks is highly satisfactory. There were identified a few vulnerabilities, which in any case are not critical and whose exploitation is relatively difficult and would require high technical skills. The only security note considerable from the security point of view regards the identification of a web application installed with little care. Such a fact is easily identifiable and could actually damage the AAA Bank public reputation since it may be interpreted as an indication of little care when putting into production mode the AAA Bank systems.

The same evalutation performed from a physical point within the AAA Bank network led to the identification of a set of vulnerabilities which are worth it to be documented due to the fact that their exploitation is quite easy to implement and the technical skill level required for exploiting them is quite low.

The aforementioned vulnerabilites may be classified into two broad categories, namely:

1. Lack of operating systems and related software update. In fact most of the identified vulnerabilities ar caused by lack of an update operation of both client and server components in AAA Bank information infrastructure.
2. Inadeguate authentication. There were found NULL passwords and/or easily guessable passwords. Furthermore, several services were found to be unprotected by any kind of authentication mechanism. Therefore whoever could actually access these services without providing any credentials.

According to the evaluation of logical and architectural aspects of the security of AAA Bank information infrastructure there exist some missing factors, and in particular this fact holds for the logical/procedural part of such a security deployment.

We are not referring neither to technical vulnerabilities nor to architectural ones. This is the case of lack of certain security features. Although such a lack does not represent a direct threat it could become the cause of various vulnerabilities if not resolved by a medium/long term security plan.

The necessary interventations in areas which are affected by security lacks are the following:

- fix, complete, integrate and spread up the security policies
- fix, complete, integrate and spread up the security procedures
- design and implement a solution capable of providing to the AAA Bank information infrastructure an adeguate level of control, business monitoring and incident handling
- define, make operational and enforce the credentials management rules
- improve and control the process of updating software
- design and implement a solution capable of providing to the AAA Bank information infrastructure a greater control over content, particularly on the internet navigation traffic.

Hacking Team deems that it is necessary to complete the performed analysis by a creating a further analysis extension being composed of the following elements which in turn have not been subject to the actual ethical hacking project:

- detailed analysis of the applications security to be performed both from within and from outside the AAA Bank network.
- security auditing of source code in highly critical software.
- a system analysis of servers which operform highly sensitive tasks, i.e. a study on the local configuration of highly critical machines).
- stress tests on web components of business applications

External Part

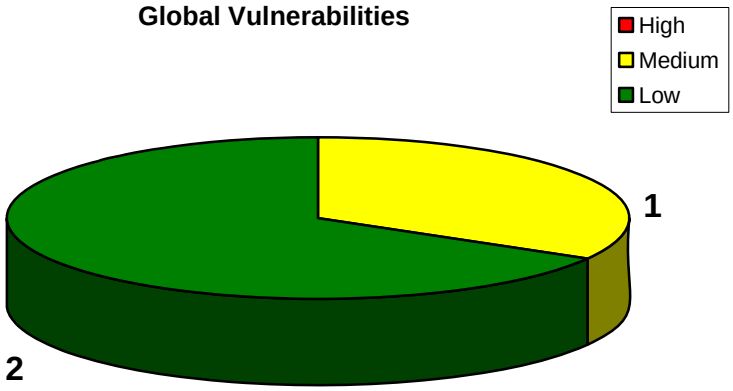

Figure 1 - Graphical representation of vulnerabilities identified acting from outside

Classification of main threats

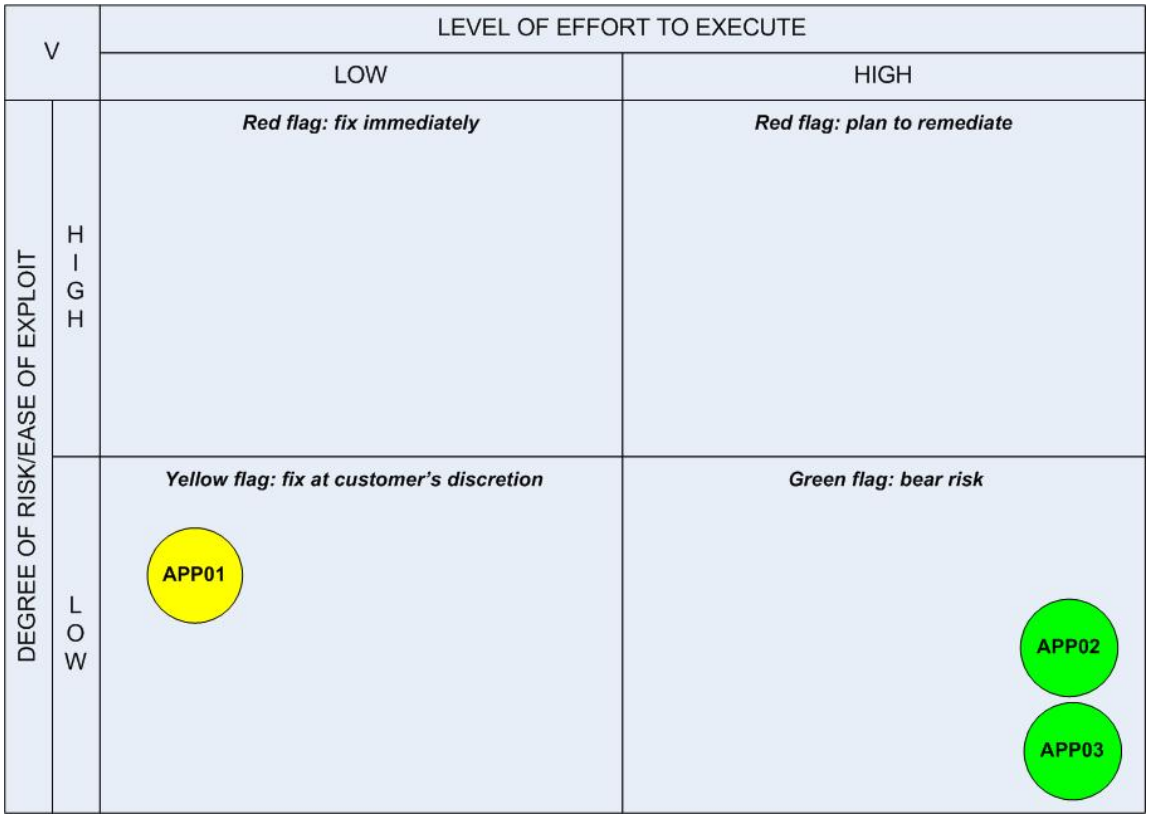

Figura 2 - A classification of external threats

Vulnerability Impact Analysis

#n	Level	Title	Description	Impact
E-APP01	M	WWW Default	Default web configuration	E' possibile visualizzare il sito web IBM di default. Non si tratta di una vulnerabilità tecnicamente sfruttabile ma un possibile danno di immagine, considerando il fatto che si tratta di una banca. It is possible to view the default installation of an IBM web site. This is not really a technical vulnerability which may be exploited. Nevertheless it may represent a threat to the company's reputation, taqking int oaccount that fact that the company in this case is a bank.
E-APP02	L	SSL V.2.0	Insecure protocol	Esiste la possibilità di intercettare il traffico in particolari condizioni unita ad una grande conoscenza ed abilità tecnica. It is possible to intercept traffic under particular circumstances combined with a high technical skill.
E-APP03	L	Apache 1.3.28	Obsolete version	It may me potentially possible to execute arbitrary code on the system. There are no known exploits publicly available. Nevertheless, the web server is known to be vulnerable to known vulnerabilities.

Table 1 - Impact Analysis on External Vulnerabilities

Internal Part

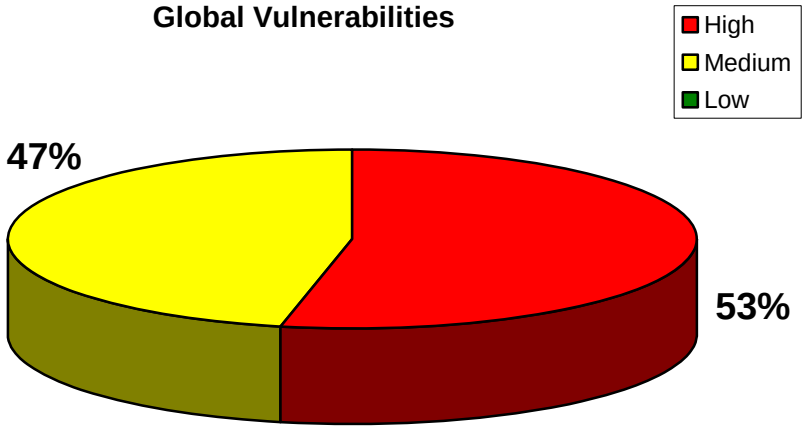

Figure 3 - A graphical representation of internal vulnerabilities

Classification of main threats

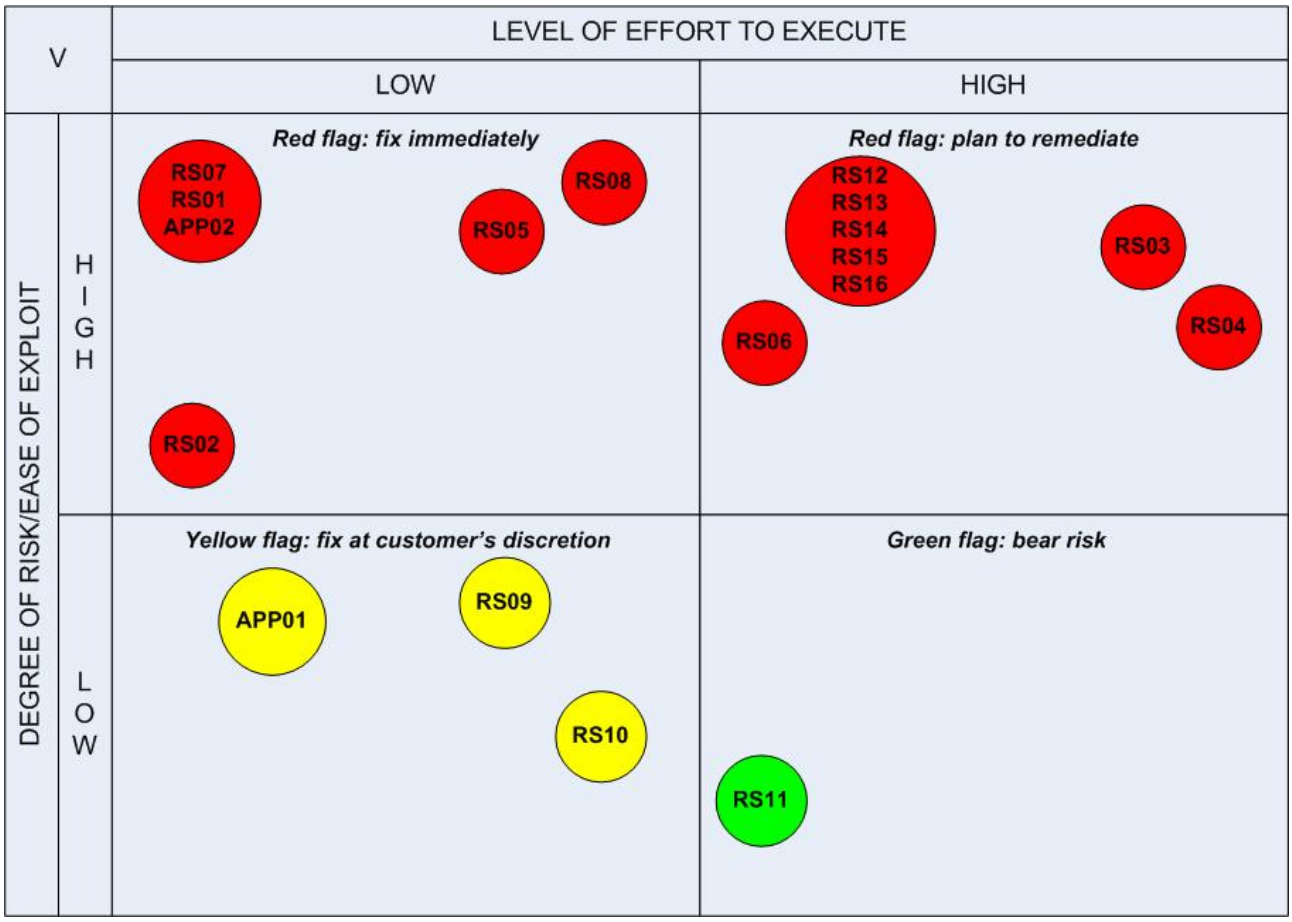

Figure 4 - Classification of internal threats

Impact Analysis

#n	Livello	Nome	Descrizione	Impatto
I-RS01	H	Lack of authentication in MySQL	MySQL data base server does not require any credentials to the *root* and *anonymous* accounts	Whoever has the possibility to connect to a vulnerable MySQL data base server coud actually access it and execute SQL queries
I-RS02	H	Lack of authentication in Oracle tnslsnr	The tnslsnr program which is the interface between Oracle clients and servers is not protected by a password	Whoever has the possibility to connect to a vulnerable tnslsnr coud actually shut it down denying service to legitimate Oracle users
I-RS03	M	Command injection in Oracle	Oracle data base server is vulnereable to malicious extensions of SQL queries	The exploitation of such a vulnerability allows an unprivileged user of a vulnerable Oracle data base server to execute SQL queries for which he is not authorized
I-RS04	M	Buffer overflow in Oracle	Oracle data base server is vulnereable to buffer overflow	An unprivileged user could gain full control on a vulnerable data base server or execute arbitrary code on the system where such server is running
I-RS05	H	tnslsnr misconfiguration	The tnslsnr program which is the interface between Oracle clients and servers is vulnerable to a design error	An attacker could write in files for which the tnslsnr has write privileges
I-RS06	H	Buffer Overflow in BrightStor ARCServe DBA server	BrightStor ARCServe DBA server is vulnreable to buffer overflow	An attacker could execute arbitrary code in a system where a vulnerable BrightStor ARCServe DBA server is running
I-RS07	H	default account in Microsoft SQL server	Microsoft SQL server may be accessed through the default account *admin* / *admin*	An attacker could access the vulnerable data base and execute SQL queries
I-RS08	H	Multiple vulnerabilities in Apache web server	Apache web server is vulnerable to buffer overflow	An attacker could execute arbitrary code on the system where a vulnerable apache server is running
I-RS09	M	NULL and Guest sessions	The system allows logons through a NULL session	An attacker could actually logon or list local users, domain usersm running srvices, shared network resources, etc.
I-RS10	H	Buffer overflow in Computer Associate License Application	Computer Associate License Application is vulnerable to buffer overflows	An attacker could actually execute arbitrary code on a system where a vulnerable Computer Associate License Application is running
I-APP01	H	Weak authentication in HP JetDirect	The administration password of HP JetDirect printer may be remotely	An attacker could retrieve the printer administration password or take full control on the

		Printer	retrieved. Furthermore, the web application which serves for a remote administration of the aforementioned printer is not protected by an authentication system	configuration of those printers
I-APP02	H	Lack of authentication in phpadmin	The web application which serves for the administration of a MySQL data base server is not protected by a password	An attacker could execute arbitrary SQL queries on a vulnerable MySQL server
I-RS11	M	Sensitive files in FTP server	In an ftp server there were found some files containing configuration data	An attacker may build parts of the actual configuration of proxies and firewalls.
I-RS12	H	Buffer overflow in Server Message Block	SMB which is a protocol for sharing files, printers, serial ports, etc., is vulnerable to buffer overflows	An attacker could execute arbitrary code in a system where a vulnerable SMB server is running
I-RS13	H	Buffer overflow in Sendmail	Sendmail mail agent is vulnerable to buffer overflows	An attacker could execute arbitrary code in a system where a vulnerable sendmail agent is running
I-RS14	H	Buffer overflow in Samba	Samba is vulnerable to buffer overflows	An attacker could execute arbitrary code in a system where a vulnerable Samba server is running
I-RS15	H	Buffer overflow in BIND	The resolver of network names and addresses is vulnerable to buffer overflows	An attacker could execute arbitrary code in a system where a vulnerable BIND process is running
I-RS16	H	Buffer overflow in Server service	Server service is vulnerable to buffer overflows	An attacker could execute arbitrary code in a system where a vulnerable Server service is running

Table 2 - Analysis of internal vulnerabilities impact

Internal Logical Vulnerabilities and Architectural Vulnerabilities

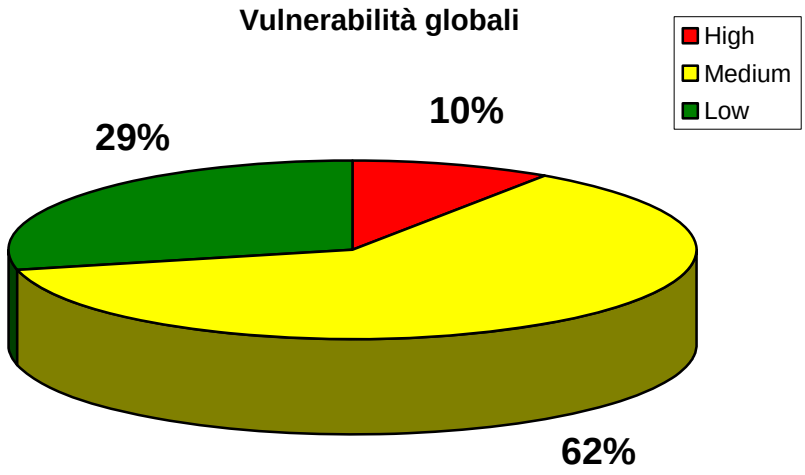

Figure 5 - A graphical representation of logical vulnerabilities and architectural vulnerabilities

Classification of main threats

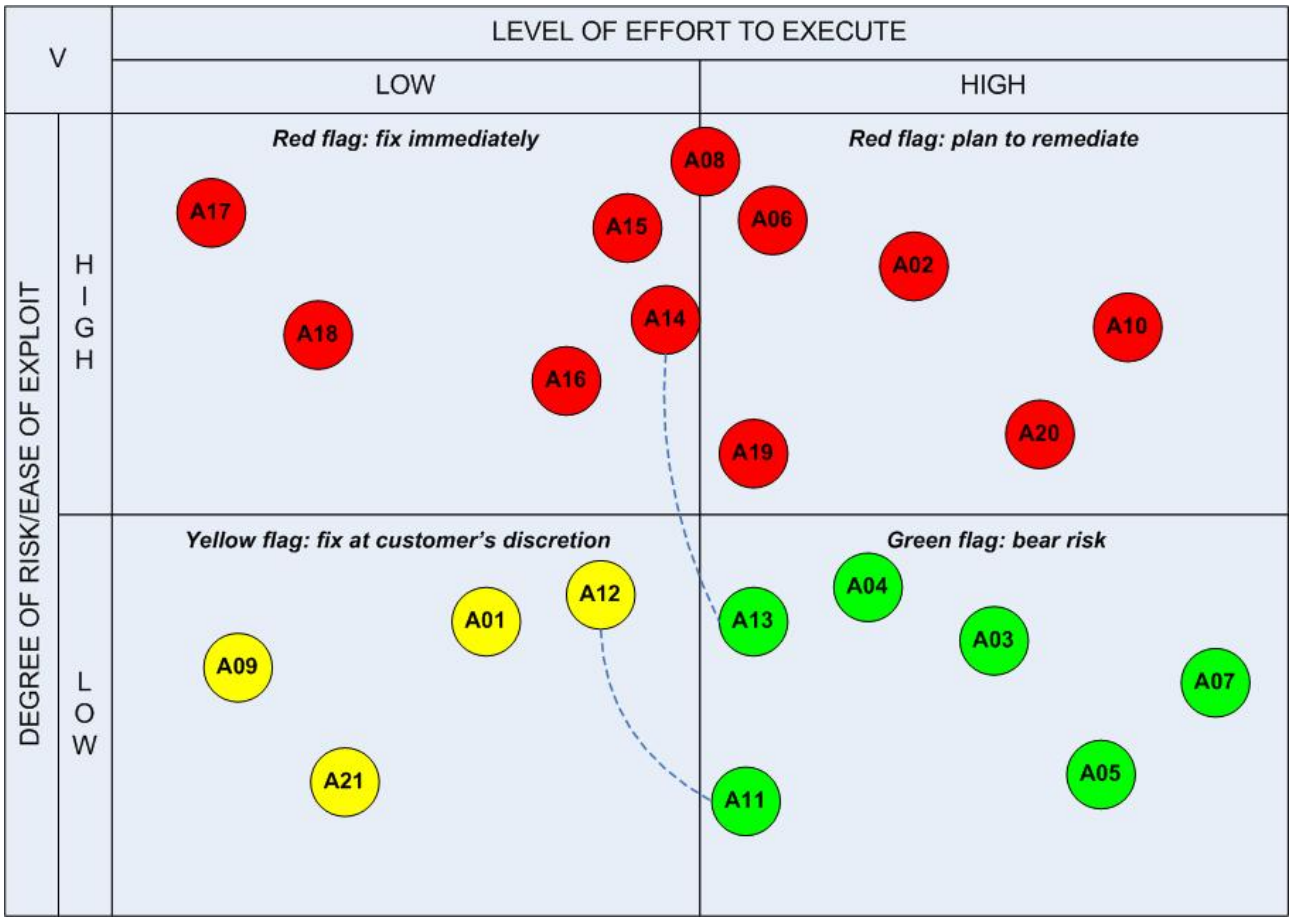

Figure 6 - A classification of logical and architectural internal threats

Impact Analysis

#n	Livello	Nome	Descrizione	Impatto
I-A01	M	Separation of accounts	There is no network separation among employees, administrators, and external consultants	Generally positioning on the same network segment users which belong to different profiles is considered a wrong practice. A user with low privileges could sniff the traffic of users who posses higher privileges potentially intercepting sensitive information.
I-A02	M	Critical servers' integrity	Critical server are properly monitored from the system administration point of view. The same from a security point of view does not hold.	Usually the attacks on a certain system cause a change of its actual state. Integrity checks on critical servers are strongly suggested.
I-A03	L	IDS	The network is not protected by an intrusion detection system	Possible security attacks against AAA Bank are neither detected nor somehow blocked.
I-A04	L	Network access	The access to a network may be achived by just changing the linl layer address of the network interface card	The decision whether to allow a device to access the network is taken upon an easily spoofed parameter. Therefore, whoever could actually access the network by spoofing the aforementioned parameter.
I-A05	L	BIOS setup password	Although employee systems are protected there is no password set for administration use.	Un utente potrebbe quindi accedere alla configurazione di base del pc e delle sue periferiche e cambiarle a suo piacimento, vanificando in tal modo le politiche impostate in fase iniziale dall'IT. A user could actually access the configuration of the machine he/she is using and change it at will. Thus, the security policies initially set by the IT personnel could be actually bypassed.
I-A06	M	Server and workstation hardening	La blindatura e le configurazioni di sicurezza su server e client sono attuate solo parzialmente e poco manutenute. Hardening and secure configuration are partially deployed. Furthermore, they are not maintained.	In front of a lack of hardening of both server s and clients they could become subject to various attacks. Thus, the security of these systems would be an evident target. After owning a critical server an attacker could deny service or access sensitive information.
I-A07	L	Web mail	No security control is performed on the	

			content of e-mails transmitted over the web.	The internal part of the information infrastructure of AAA Bank is not protected by malware being transferred through web mail. The defense from such a threat then is left on client security mechanisms, fact that often results to be insufficient.
I-A08	M	Secure net surfing	No security mechanism protecting the internet surfing is activated.	The web surfing practiced by employees is subject to amost of the actually known attacks, namely trojans, backdoors, spywares. This fact would cause a damage to a client machine. Furthermore, it would transform an extrnal attackm into a new one since now attackers control a machine located within the target network.
I-A09	M	Strong Authentication	Remote access is enabled, but it relies on username/password authentication.	Any remote access of both employees and externals is carried out through a VPN, but the authentication to a service is performed through a weak mechanism, namely username/password. An attacker who makes it to acquire such credentials could impersonate a legitimate user and access all resources to which the victim user is authorized to access according to his/her profile. A two-factor authentication, namely something one knows and something one has, should be applied to control access to critical resources.
I-A10	M	Encryption of data in lap tops	There is no encryption mechanism of data stored on lat tops and other company systems.	In case of theft of lap tops all critical data which reside in them could be easily accessed by an attacker.
I-A11	L	Patch verification	Tests on configuration changes and update of software are performed on servers while in production	On of the most important procedures in IT is represented by the one utilized for the update of software and configurations. A vulnerability in such a sense could actually leave servers in an unprotected state. Thus, it could expose servers to attack along with consequences such as dysfunctions or becoming an attack point.
I-A12	M	Deployment patch and variations	A positive test on servers in production is assumed to be such on the remaining systems	
I-A13	L	Trackability of provisioning	There is no recording process related to acces privileges assigned throughout the time	There is no efficient and secure control on access privileges granted on critical resources. The task of managing employees identities has become quite important in nowadays companies

I-A14	M	De-Provisioning	There is no adeguate control on inactive accounts	
I-A15	M	Monitoring	There is no event monitoring mechanism which are of security concern.	It is quite dangerous to have a false sense of security: nothing happens if we are not aware of it. Without an adeguate monitoring system dedicated to the most critical and sensitive business part we cannot known what really occurs from the security point of view.
I-A16	M	Log centralization	La centralizzazione dei log è effettuata solo per gli eventi relativi alla parte firewall e navigazione. Il loro controllo è effettuato saltuariamente (solo a fronte di problemi emersi) e manualmente. Log centralization is applied only on firewalls and the web surfing part. Possible controls are performed casually and the interventions are done manually.	Centralizing at a unique point the various security related logs is a common correct approach. Such an approach however should be well evaluated before being applied for the purpose of avoiding the lack of centralization of important information or centralization of useless information.
I-A17	H	Security operations center	There is not centralized security system which may be used for correlation Operations of business events, alarms,	In the case of companies to which security is highly important (or is considered to be such) it is more and more important to possess a system which allows for: centralizing and preserving network security events, system security events, and application events which are strictly related to security

			incident handling, reports, etc.	o centralizing and preserving network security events, system security events, and application events which are strictly related to security, o perform a correlation of information related to business activities, o provide a query system to be utilized for event retrieval, o communicate to the people in charge in deviation to the predefined policy o provide an alarm and incident handling service, o provide a reporting service for internal use, legal use, or legislative use.
I-A18	H	Security policie	The security policies are not official and complete. Furthermore, they have not been properly distributed.	As there is a lack of approval and correct distribution of security policies, there are no rules to respect. Without certain rules everyone will act as he/she deems appropriate, or not act at all. Among the most used security policies there are missing the most important ones such as risk analysis, business continuity, sensitive data treatment, incident handling, utilizing company resources, cleandesk, education, etc.
I-A19	M	Security procedures	Security procedures are not well written and complete.	Partially due to I-A18 actually deployed security procedures represent a small part of the security procedures which should be in place in a company where information security is an important factor. Furthermore, the actually existent security policies have been written without the awareness which makes them usable, readable, distributable, by for example any just employed IT employee.
I-A20	M	Firewall management positioning	The server utilized for managing firewalls is placed in an adeguate zone (DMZ).	The DMZ is usually a network zone populated by services offered to external clients. Therefore it is not a good practice to place at the DMZ zone the systems used for managing internet security devices. If an attacker could actually take control over such a network zone then he would be able to control the aforementioned managing systems
I-A21	M	Optimization of firewall rules	The firewall rules are not optimized and well structured.	A set of well structured and clean rules is more secure and more immune to possible errors: o facilitates debugging operations, o facilitates the performance and efficiency of devices, hence the speed of transmission, o facilitates the insertion/deletion of rules, and generally the overall system management.

Tabella 3 - An analysis on the impact of logical and architectural internal vulnerabilities