Department of Software Engineering and Computer Science
DABX36 – Bachelor thesis
IADP Third year, spring 2001

Application Service Provider – A viable solution seen from the customer's point of view?

Authors: Buket Ukus, ia98buk
Kaarina Tejle, ia98kte

Course examiner: Gouhua Bai
Tutor: Birgitta Hermansson

Abstract

An Application Service Provider (ASP) is a company that offers individuals or enterprises access over the Internet to applications and related services that would otherwise have to be located in their own personal or enterprise computers. The simplest way to understand the ASP concept is to think of it as "application-renting". However, the customer always owns the data.

The primary purpose of this thesis is to see what kind of demands there is on an ASP solution from the customers' side. The secondary purpose is to see if the customers could consider an ASP solution if their demands were met. We have also given an explanation of the ASP concept and what factors, within the data security context, makes the solution acceptable among customers.

The method we have used to find a result to our hypothesis and research questions, is that we have collected different text materials and conducted interviews. The interviewed companies where four ASP suppliers and four future possible ASP customers.

The result of our investigation showed that a majority of the interviewed persons could consider an ASP solution. The result could however not be estimated and applied for the entire company, because of the variety of knowledge between the different departments.

The ASP industry is clearly in the stage of maturity within the IT business, but it seems like the psychological barrier may be the strongest factor that can diminish the success of ASP.

Acknowledgement

We want to extend a big thanks to our tutor Birgitta Hermansson and our examiner Guohua Bai, at Blekinge Institute of Technology, for the support and encouragement we have received during the process of writing this thesis.

We also want to thank our supervisor at Jobado AB, Tony Gorschek (CTO system architect), for our lively discussions, great feedback and support.

A special thanks to the people at Europolitan AB, Flextronics AB, the Municipality of Karlshamn, and Symbian AB for spending time with us despite their busy schedules. We are very grateful and without them our thesis could never have been written.

Also a grateful thanks to the persons at Iterium.net, PEBS AB, and Sema Group AB, for participating in our investigation, by giving us the suppliers point of view.

Ronneby May 21th, 2001

Buket Ukus *Kaarina Tejle*

TABLE OF CONTENTS

APPENDICES

1. Introduction

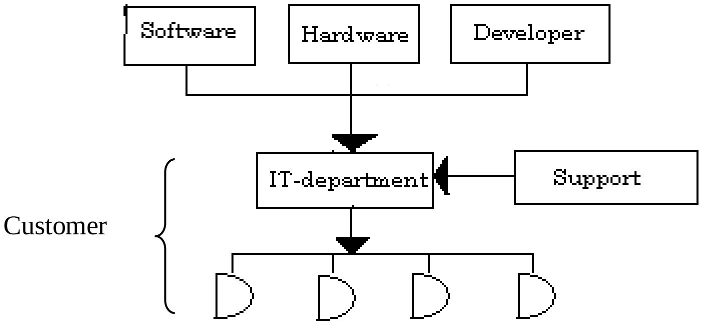
1.1 Background

The idea behind the possibility to hire specialists for the areas that your own company is not good at, has been around for some time and started in the 70's, where it was implemented in the, so called, service bureau [SE00]. The service bureau stood for the possibility to outsource functions in the primitive form. About ten years ago the modern concept of outsourcing and ASP started to take form.

The modern concept of outsourcing and ASP has become more popular now when we are entering the, so called, learning society where the key words are "main business", which means to concentrate on what you know best. Application service Providers solve a key problem that companies of all sizes have been grappling with for years: how to take advantage of the best software applications on the market without hiring expensive specialists, without waiting for lengthy deployment cycles, and without compromising on quality [SM01].

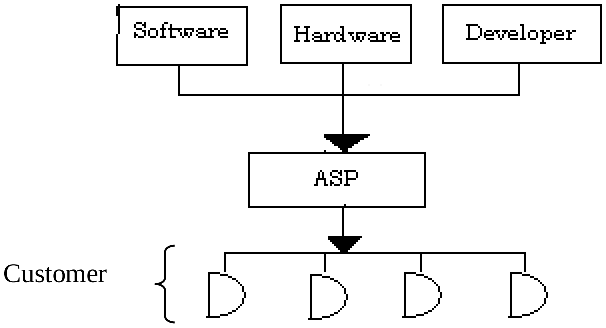
An Application Service Provider (ASP) is a company that offers individuals or enterprises access over the Internet to applications and related services that would otherwise have to be located in their own personal or enterprise computers. The simplest way to understand the ASP concept is to think of it as "application-renting" where the application is often custom-tailored to fit a company's needs. The customer can, for instance, rent an application system from a company, use it for 1-2 years and then decide to change the service. The customer can store everything from customer records to company information, that from here on will be called the data. The data that is stored, is owned by the customer and is given back or deleted when there is no need for the system. The advantage is that the customer does not have to worry about the hardware, software, bugs, backup or security, as the company that provides the service will take care of these matters.

The traditional concept of outsourcing (See picture 1.1) means that a company turns to an outer source for applications and additional network environments [SE00], but the customers' hardware and local area network stays at the customer and is supported there. The outsourcing company comes to the customer to give support and updates.



Picture 1.1: Outsourcing in relationship to the customer

To separate outsourcing from ASP (See picture 1.2), ASP is also called outhosting [LB00]. The significant difference between ASP and outsourcing is that when using the ASP solution the hardware for the solution is relocated at the ASP and the customer can reach and use the application with help of thin clients. In most cases a web browser is used as a thin client.



Picture 1. 2: ASP in relationship to the customer

Within the ASP concept you can see two main lines of directions, the fully managed ASP and the co-location [JLR01]. With the fully managed the concept is built on the fact that the ASP suppliers handle everything that includes administration, support and hardware storage at their own location.

With co-location the customer handles the administration and support but at the location of the ASP supplier. The hardware is located in the ASP supplier's buildings and the customer usually accesses the administration tool through secured connections.

1.2 Context

Our investigation will attach great importance in understanding why customers are expected to be interested in using an ASP-solution. What do the customers require? Necessary areas like security, reliability, availability, performance and adaptation will be taken into consideration and examined to find the preferable data security solutions that would please the customers.

To be able to accomplish our thesis we will co-operate with a company called Jobado AB, which is located in Ronneby, SoftCenter. Jobado AB is a newly established information agent on Internet. With its concentration the company has a unique position in Sweden. The basis of their operation is to collect, work up, store and supply information, and make it available for the Recruit-, Freelance- and Staffing markets [JOB01].

Jobado acts as an intermediary between these markets to ensure that the communication and contacts are successfully made. Jobado provides an ASP solution for internal recruitment, which means to benefit from existing workforce. Therefore the internal recruitment solution will be mentioned in the interviews and analysis of interviews.

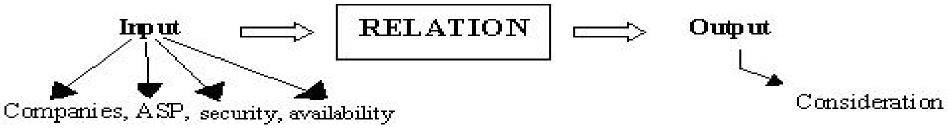
1.3 Method to find solution

1.3.1 Hypothesis

To get the right angle and focus on the report, we have formulated following hypothesis, which the result of our report will be based on.

"Companies are willing to consider an ASP-solution if certain demands are met. This includes demands on security and availability."

We have stated some input and output variables to help us come to a result, where the relation is that the inputs are independent (of the output) and the output is both measurable and dependent (on the input) (See picture 1.3).



Picture 1.3: Input and output relations

1.3.2 Clarification of input and output variables

"Companies"
Possible future ASP customers that have more than 500 employees and that can consider an ASP-solution in the future.

"ASP"
An IT-solution that makes it possible for companies to rent an application that is available via the Internet. In this case, the ASP-solution is also associated with the recruitment-system that Jobado AB is providing.

"Security"
Data security that should consider integrity, storage and confidentiality to protect data from being altered, destroyed or misused by intruders.

"Availability"
The assurance of high quality service of accessing unaltered data.

"Willing to consider/consideration"
The ASP-solution is an alternative to be used within companies and can be measured in three grades that we have defined ourselves:

- Interested, and want to test it.
- Interested, but want more information.
- Not interested.

1.3.3 Research questions

The following questions will be answered while testing the hypothesis:

- Is ASP reliable concerning storage of information?
Here, we have paid attention to the data storage aspects ASP suppliers provide.

- What is expected from an ASP-solution to be trusted by customers?
What does the ASP-solution have to live up to according to the customers, concerning data security and availability? What is, from the customers' point of view, necessary and expected from the ASP for achieving high security?

- How can the security level within an ASP-solution be determined for the customers?
Which process do the ASP suppliers go through to determine the security level for the customer?

1.4 Purpose

The purpose of writing this study is to see what kind of demands there is on an ASP solution. ASP is a new word for an old practical solution to the problem of not having enough knowledge or investing money for a specific needed division of a company.

This thesis will show why, or if customers would choose an ASP solution and what thoughts there are around it. It will also give an explanation of the concept ASP and what factors, within the data security context, makes the solution acceptable among customers.

This report will additionally work as a ground for further customer contacts for the company Jobado AB.

1.5 Target group

The target group for this study is in the first place Jobado AB that is interested in what possible future customers think about ASP and the company's specific recruitment system, provided as an ASP-solution. ASP suppliers, who have not investigated in what customers want, believe and expect from any kind of ASP-solution, should also benefit from this report.

We also turn ourselves towards the possible future customers who might need further explanations of the concept and the definition of ASP.

1.6 Goal

The goal for this study is, first and foremost, to have an investigation that shows what kind of demands the customers have on an ASP solution.

Also by trying to prove our hypothesis we will give a larger picture of the concepts of computer security and availability within the ASP area, both from customers and suppliers point of view.

1.7 Delimitation

1.7.1 Logical management of data

Security is one of the key inhibitors to ASP success. A secure computing environment can be very complex. As it involves a great number of aspects it is impossible to take them all into consideration in this report. Therefore we have limited the security area to include only the logical management of data security within networks, which means:

- The three central goals in computer security: confidentiality, integrity, and availability [ET98].
  Confidentiality: *protection of data so that it is not disclosed in an unauthorised fashion.*
  Integrity: *protection of data from being changed or destroyed in an unauthorised way.*

Availability: withhold of unaltered data and the management of network interruptions.

- Firewalls: what are firewalls and how important are they in the context of data security?
- Secure data storage: backups.
- Risk management: is mentioned briefly, as it is an important process of determining the right security level for the customer.

Issues like human threats within the ASP organisation that could result in loss of confidential data and protection of physical objects are of high importance, but we have decided to exclude these areas in this report. We do not cover security products either, as we think that the overall theory and concept of data security is more important than the very fast development of products, which changes several times a year. This means also that the technical points and details are not covered.

1.7.2 Outsourcing and outhosting

In this report, we have concentrated on the data security aspects within outhosting, as we are not looking after comparisons between outsourcing and outhosting. This means that our investigation will be focused on the ASP-solution where:

1. The application is installed in a remote facility that is not owned, managed, or protected by the customer's employees.
2. All access to hosted applications occurs over the Internet.

1.7.3 Companies to be interviewed

The delimitation of customers is restricted to companies that have more than 500 employees. If they have an IT-department or not is not of importance.

We have no restrictions concerning the suppliers, as we think that the size of the ASP-companies should not matter, because they all have the security aspects as their main reason for survival in the business.

2. Method

2.1 Material

We have used three forms of materials: text material that includes books, Internet pages, articles and other exam thesises, material received at the IT-conference we visited in Stockholm on the 5th of April and material from interviews.

2.1.1 Written material

The written material we used was collected from the two libraries in Ronneby and where in areas based on these search keys:
”Internet security”
”Data integrity”
”Infrastructures”
”Standard systems”
”Firewalls”
”ASP application service provider”

None of the written materials are very technical but more towards the area for the logical management of data security. Especially all the articles are from real world experiences and concern everything from business relations to ASP definitions.

For full list of references and other literature, see chapter 7 and 8.

2.1.2 IT-conference

4-5 April, there were a professional IT-conference and exhibition in Stockholm (Sollentuna Exhibition Centre), called e-Business Software and Information Management.

Information Management is the only expo in Sweden concentrated entirely on digital information services and information management systems. e-Business Software is Sweden’s premier administrative business systems and e-business expo [ECE01]. The arrangement was designed for IT managers, accounting managers, and high-level decision-makers in the private and public sectors.

We heard about this event through a friend. When we realised that exhibitors would not only show everything from information systems and business intelligent to the latest tools for efficient administration, but also have lectures in ASP and IT-security we decided to attend the event.

5th of April, we were present at a two-and-a-half hours long lecture, which was hold by Telia AB, KPMG Consulting AB and IFS. The main presentation was about the ASP concept as an IT-solution, the business opportunities it provides, risks and the economical aspects. From this lecture, we got a broader knowledge and understanding of how ASP is used and regarded in real life businesses.

By participating in this exhibition, we also took the opportunity to get into contact with ASP suppliers, which we later on interviewed.

2.1.3 Interviews

The interviews we have done are divided into two parts. We have interviewed both possible future ASP customers and also companies that have their IT-operation and IT-security as their main business, in other words ASP suppliers.

Why we have chosen to interview ASP suppliers is because we wanted to use their answers as a complement to gain further information about data security requirements both from the customers and suppliers point of view.

2.1.3.1 Customers

Companies that we have looked at as ASP customers are Europolitan AB, Flextronics AB, the Municipality of Karlshamn, and Symbian AB.

The reason why we have interviewed companies that have more than 500 employees is that we wanted to look at the general thoughts about the system Jobado AB is providing, which probably would not be too much of a use for smaller companies.

To find and get into contact with companies were totally under our responsibility. We solved this problem with personal contacts, e-mail and phone calls.

Within each ASP-customer, we have interviewed people from three different departments. The basic idea was to get a general picture of what companies think and know about ASP, its data security and what would make them chose an ASP-solution. We have interviewed one employee from the IT-department, who takes care of the data security aspects, a person or persons within the personnel department, who could use the recruitment-system in recruiting purposes, and one regular employee, who would store his/her information in the system.

The questions were formulated quite similar, but with some adaptations depending on which department we were going to interview. Why we needed to make such an adaptation was because we wanted to angle the questions not only to the ASP-solution and data security, but also towards the recruitment-system that Jobado AB is providing.

All of the interviews, but Flextronics AB and Symbian AB, were done orally by visiting the companies. Each interview took between 30 minutes and 1 hour, depending on the knowledge the persons had in ASP and data security. We realised the interviews with Flextronics AB and Symbian AB via e-mail.

2.1.3.2 Suppliers

The companies we came into contact with through the IT-conference and who took part in our interviews were Iterium.net and PEBS AB. Iterium.net is Sweden’s biggest ASP-supplier and PEBS AB’s main business is to provide flow- and process oriented IT-support.

Jobado AB, that we are co-operating with, and Sema Group AB, which is one of Sweden’s leading companies specialised on IT-services, were the other two companies that we interviewed.

We did the interviews via e-mail because that would be the most convenient method for both parts, either the reason was time or distance. However, as Sema Group AB is also located in Ronneby, we could carry out our interview orally at the company.

We did not need to make any adaptations concerning the questions, as the employees all work professionally with security aspects.

2.2 Procedures

With the found written material we have formulated our interview questions and gathered theories around the specific selected areas within ASP.

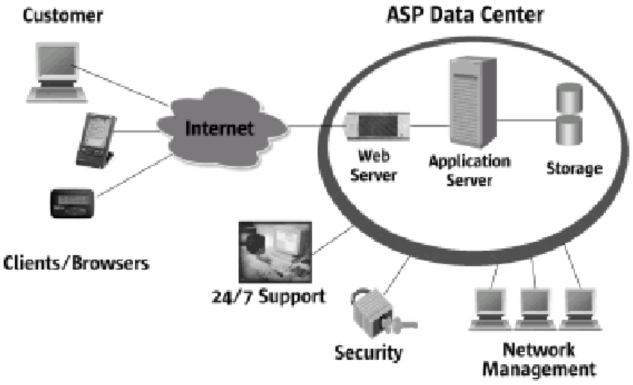
The materials we have used from the interviews are answers given to us from the four ASP suppliers and from the four ASP customers. We have put together the interviews from the suppliers, as they are from our point of view considered as facts, and drawn parallels between the written theories and the answers. The answers from the customer interviews have been analysed separately as they are very varying from department to department. The result from both theories and interviews helped us to identify and clarify the data security aspects within ASP and answer our research questions.

3. Information review

3.1 General Infrastructure of ASP

The service delivery infrastructure for ASPs usually includes certain key components as web servers, application servers and database servers [SM01] (Se Picture 3.1).

The web server is used for hosting the web site and providing an interface for browser-based access to applications and data. The application server houses the applications that the customers are hiring. The database server stores and provides the access to the data, files and information requested by the application or web server.



Picture 3.1: ASP architecture [SM01]

There are two different models of infrastructure for hosting applications for multiple customers. They are called physical separation vs. logical separation, which refers to how many customers that share servers [KA01]. In the physical separation model each customer has its own server/servers dedicated to only this customers traffic and business. With the logical separation approach, several customers share one or more pools of resources from the ASP.

The customers' tendency to prefer the physical separation model has to do with giving the customer peace of mind and higher perceived security. It is also considered to be the safest one. Though, it is rarely used due to its possibility to cause infrastructure scalability issues.

The ASP suppliers prefer the logical separation model due to its management simplicity, flexibility, and resource utilisation.

In the end no matter how the ASP is structured the ultimate objective is a seamless service in which the customer interacts only with the ASP [SE00].

3.2 Data security

Data security includes control of data access, continuous backups, management of network interruptions, and encryption of outgoing data. The aim is to achieve among other things confidentiality, data integrity, and availability [KP96].

When hiring an application from an ASP supplier, the customer looses all control of data. The interaction with the application from the Internet makes it more difficult for customers to rely on security, as the Internet does not provide a secure network transport by default. The logical security problems cause more than twice as big damages as the physical security problems [KP96]. The reason is that the logical threats like hackers, virus, network interruption/delay, and wiretapping are more diffuse than other problems and therefore more difficult to manage.

When people are asked why they think computer security is important, their responses usually show concern for confidentiality [ET98]. Integrity of information is also of concern in everyday life. The interviews we made with customers showed actually the same concern factors when relating to an ASP-solution. For this reason the ASP suppliers must be considerate of the unique requirements that each of their customers have, while still maintaining a secure computing environment [SE00].

Today, all of the interviewed suppliers configure technically the security of their customer’s data with help of firewalls, VPN, encryption, storage, backups, and SSL.

3.2.1 Firewalls

A firewall is a device (usually a computer running a specially written or modified operating system) with a single task: to isolate an organisation’s internal network and traffic from the Internet at large, allowing specific connections to pass and block others. Firewalls are configured so that all outside connections to an internal network go through relatively few well-monitored locations. In so doing, firewalls are part of an organisation’s overall security strategy.

Firewalls are a security solution with the purpose to prevent unwanted and unauthorised communications into or out of the ASPs’ protected local network. There are however at least two types of security problems that firewalls cannot address [ET98]:

- Generally they do not provide protection against insider attacks. An insider can still steal critical info or damage Intranet resources. This threat can be addressed by implementing appropriate authentication, authorisation and access control mechanisms inside the firewall. Additionally Intranet firewalls can be used to reduce the risk of insider attacks.

- They do not provide protection against data driven attacks such as virus-infected software and files. This problem must be handled with both policy and some dedicated antiviral software controls.

The interviewed suppliers all agree that a firewall is a condition for achieving security between the internal and public networks. But they also make it clear that a firewall alone does not provide high security if the traffic is not monitored, the security weaknesses addressed by additional applications, and the firewall upgraded.

The ASP suppliers should not be lulled into a false sense of security because of the fact that they have a firewall. A company should realise that firewalls should only be used to gain additional security that works in conjunction with internal controls – and never as a replacement for them [GS97]. To install the best solution, IDSs (Intrusion detection systems) should be used to scan problems and detect intruders in real time [ET98].

“If the firewall is properly configured and contains no serious bugs, the network will be as free from risk as possible” [SP00].

3.2.2 VPN

The security problems of today are most effectively solved with firewalls and Virtual Private Networks, also called VPNs [SP00]. A VPN that is strongly encrypted is necessary for offering dedicated, secure paths or tunnels, to reconcile the public nature of the Internet infrastructure with the need for security to facilitate e-Business [SH00].

A VPN is not encrypted by default, but consist of the option to authenticate and encrypt tunnels over the Internet. It makes a portion or perhaps, all the transmitted data invisible for external observers. The data is encrypted and therefor cannot leak out during transmission, unless the located on the other end has the proper key to decrypt it. However, even if a VPN provides authentication it is not as strong as having the user directly identify himself or herself to the person on the other end but it does provide a reasonable level of authenticity [SE00].

The usage of VPN is very popular among the ASP suppliers. The level of security depends very much on the customer’s requirements on privacy. However, if the requirement for privacy is high, then there is a corresponding requirement for strong security of access and strong security applied to data passed over the common network. If a customer is very interested in authenticating a transmission, then a digital signature would be a beneficial security feature to implement [SE00].

3.2.3 Encryption

Much of the attention that is paid to web security involves the problem of protecting information from unauthorised interception as it travels over the Internet. In addition to firewalls and VPN’s, authentication is a key component of any ASP security scheme [MM00]. There are many ways to protect data from eavesdropping or unauthorised people from capturing and corrupting it as its travels through the network. However, encryption is the only one that is practical [GS97].

Encryption is the process of turning a clear-text message into a data stream that looks like a meaningless and random sequence of text. It is used to make data unreadable before, for example, transmitting it over an insecure network like the Internet. Encryption can be used to protect the following types of network data:

*Private communication containing sensitive information.
*Secure file storage, such as data on a hard drive.
*User or computer authentication.
*Secure password exchange.

Many identification systems can be improved through the use of digital signatures. The theory behind digital signatures is based on a private and a public key, where the private key is used for signing one's signature to the block of data and the public key is used for verifying a signature after it has been signed.

The advantage of using public key cryptography is that this proof can be done safely over a computer network, even if a third party is eavesdropping. Public key cryptography is one of the systems that offer the best hope for sending secure, authentic electronic messages over open networks [GS97].

Security professionals have identified four keywords that are used to describe all of the different functions that encryption plays in modern information systems. The different functions are these:
Confidentiality: Encryption is used to scramble information sent over the Internet and stored on servers so that eavesdropper cannot access the data's content.
Authentication: Digital signatures are used to identify the author of a message; people who receive the message can verify the identity of the person who signed them. They can be used in conjunction with passwords or as an alternative to them.
Integrity: Methods are used to verify that a message has not been modified while in transmit.
Non-repudiation: Cryptographic receipts are created so that an author of a message cannot falsely deny sending a message.

To be able to offer confidentiality, authentication, integrity and non-repudiation to their customers, the suppliers need to use the technique of digital signatures and/or other kind of encryption methods.

3.2.3.1 SSL

One of Netscape's Communication's early innovations was its Secure Socket Layer (SSL), a system for automatically encrypting information as it is sent over the Internet and decrypting it before it is used. The real promise of SSL, is to provide secure administrative access to web servers and to allow businesses to transmit proprietary information over public network, which also means to provide data confidentiality and data integrity.

SSL is a layer that exists between the raw TCP/IP protocol and the application layer. It does a good job protecting all communication while the data is in transit and gives the users good assurance that they are communicating with the sites they think they are.

Many customers wonder if it is safe for their data to travel over the Internet. All communication to and from the ASP should be over encrypted lines of communication. Secure Socket Layer is the most popular method for delivering encrypted web pages [KA01].

However, this does not mean that SSL alone is enough for securing the data flow between the suppliers and the customers. According to one of the suppliers, SSL does not provide a high encryption level, even if the highest amount of bits (128), that is allowed according to the agreements between USA and other countries, is used. Today, computers are very strong and can crack a 128-bits encryption. Some of the interviewed suppliers pointed out that beside SSL there should also be methods for signing the data and/or encrypting the data to assure higher level of security.

3.2.4 Security considerations

An ASP must provide a secure environment for the customers' data. How secure it will be is up to the customer' s requirements. According to the suppliers, there is no solution that could be called the perfect system architecture. How well a security solution is configured depends on many factors. The customers' demands on, for example, the security level of the data that is transmitted and stored at the ASP suppliers, the data and system access policy formulated by the customers and how much the investments on the security will cost, makes a big difference from solution to solution. The best solution for the suppliers is the one that the customers need and want.

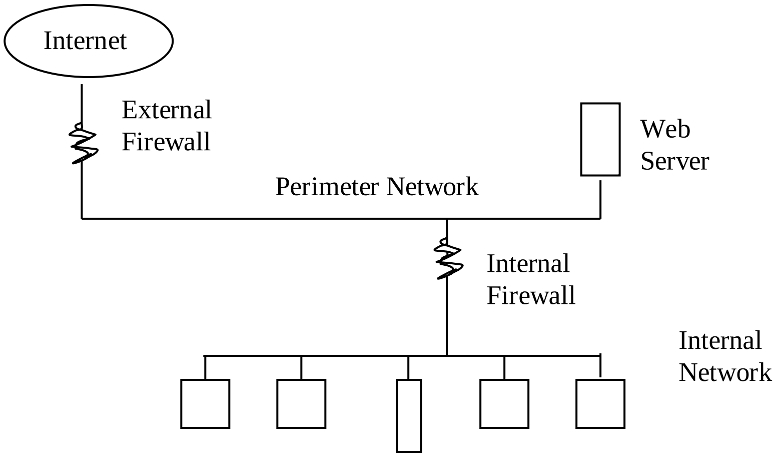
The application that will be used plays a central role as well. A word processing program does, for instance, not require as much security as a patient journal program. It all depends also on how you access the application. Is it from the company's local area network or is it from any machine that is connected to the Internet? If it is from a company's own network, some of the access control problem could be solved, for example, by restricting the computers that have access to the ASP application only to those that are within the company. This is however usually not preferred, as the application cannot be reached unless the user is in the company.

Under the ASP model, all data is confined to a server environment. As it is easier to protect servers than client devices, this method is more secure [SC01]. The client devices are also less vulnerable to theft because the application is not installed locally.

When user’s access request is to an application object, the access control rules are evaluated in the context of that application and not by the operating system. Making the application available for authorised users is according to the suppliers quite simple. In this case, the access control is typically based on the validation of the user’s login and password against a database, not the identity of the computer that the user is working on.

3.2.4.1 Firewall

The importance of how to place the firewalls is significant, because according to one of the interviewed suppliers, both the software and hardware needs protection against external attacks. A preferable solution could be the use of several firewalls with different tasks. For example there could be use of two firewalls: one to shield internal network and one to shield your web server (Se Picture 3.2).



Picture 3.2: A web server located between an internal firewall and an external firewall.

The advantage of locating the web server behind the firewall is that the firewall will block outsiders from using other Internet services, such as Telnet and FTP. However, if attackers manage to subvert the web server through for example a faulty CGI script, they will have full access to the internal network [GS97]. Having the web server outside the firewall would not be an advantage since the web server will not benefit from the protection the firewall affords.

3.2.5 Storage

To store the data within the ASP suppliers deploy a wide range of storage architectures depending on their customers' requirements. The storage hardware may be directly attached to the servers or they may be pooled via a storage area network (SAN). Directly attaching the storage hardware to the servers may be more cost effective, but harder to manage. On the other hand the SAN solution is more effective when using the resources, but can prove to be more technical complex.

An ASP company should only use a third-party co-location facility because that is the most secure way for serious ASPs to protect their customers data [KA01]. Co-location facilities offer physical security such as restricted building access, fire protection and locked cages.
The consulted suppliers both store the data in so called SAN solutions and directly attached to the servers. They implement both the solution to physical separation of the customers data and not, depending on the customer and their demands.

3.2.6 Backups

A backup is simply a copy of data that is written to tape or other long-term storage media. Backups serve many important roles in web security [GS97]:

*Protects the information during equipment failures.
*They protect the data if accidental file deletion occurs.
*They protect from loss of data when break-ins occur, as files that are deleted or modified by an attacker can be restored from a backup.

One important thing to remember is that you must verify that the data on the backup is intact and can actually be used to restore a working system.

Good routines for backup can eliminate many problems from a computer system. Work copies, security copies and machine content are minimum demands on what is necessary [KP96]. Backups should be taken as simply and regularly as possible. Inflexible and non-automatic routines lead to neglect.

To achieve good routines for doing backups you have to have a backup plan, where it must say [LB93]:

*What should be copied and why?
*When should it be copied?
*How shall the copies be stored and protected?
*Who has the responsibility for it to be done?

Another important aspect is to be sure to locate the security backups in another physical location, away from the regular servers [KP96].

All the consulted suppliers name backups as one of their main solution to preventing data from being changed or destroyed. The normal routine is to have a daily backup, which then goes into a weekly backup, which in turn goes into a monthly backup.

How fast the data can be recovered depends entirely on how much data it concerns. All suppliers name tape as the way of having backups. “There is no alternative way today”, is their response. A couple of the suppliers also take measures as having mirrored records fore the most important data. One of the suppliers points again out the importance to check the backup, so that it is up to date and usable.

3.3 Availability

Seen from the users point of view there are three main types of demands on availability [LB93]:

- Answer time, how long and how fast the information system can leave an answer to a given question.
- System availability, which refers to how long and how often an operational interruption can be aloud to occur under normal operational conditions.
- Maximum inactive operational time, what is the demand on how long the system can be allowed to stand still in connection to a situation classified as emergency.

Operational interruption is the Achilles’heel for an ASP supplier, and an interruption can bring catastrophic consequences for a customer’s company [KP96].

In order to provide their customer with the availability they have promised, an ASP must be able to respond to emergencies [SE00]. Availability services often have to include guaranteed Internet bandwidth connections, backup generators and fire suppression systems.

If the ordinary line is corrupted it is good to have an Internet solution with a reserve line to another Internet operator [ÅB01]. All the contacted suppliers have some kind of backup line for their Internet connection. They also all guarantee a high percentage of availability when not considering external error that is not within their responsibility area.

The factors that control the availability from the ASP suppliers’ point of view are the local environment at the customer, the external communication connection to the ASP supplier and the environment at the ASP supplier. If you disregard server breakdown the most occurring error concerning the availability lies at the customers Internet connection.

To secure availability as an ASP supplier you can, for example, build double rings, redundancy in different manors and prevent the components from be exposed to disturbances. Since it is almost impossible to entirely prevent disturbances that will affect the availability also rebuilding actions, like backups, sparepart holding and catastrophe plans should be prepared [KP96].

3.4 Risks

When looking at the risks involving ASP, you first have to consider the fact that risks like natural occurring phenomena, cutting of a cable, or any other line disruption that is not in the hands of the ASP suppliers. These interruptions might annoy the customers, but they cannot really be helped.

Web security is not “all or nothing” – security is a matter of degree. The more security measures you employ, the more you reduce your risk, but this also leads to diminished usability. The goal should be to reduce risk as much as it is practical, and then to take additional measures so that if there is a security incident, you will bee able to recover quickly [GS97].

For the ASP suppliers, security risks come in two forms: external, or threats from outside the company or its ASP; and internal, or threats from within. Insider attacks has been more prevalent and damaging. The insider knows where the good stuff is and also may have the motivation to do something to hurt the company. But as people put more valuable resources up on the Internet, the outside attack becomes more expected.

ASP decreases the risks for intrusion since everything of value is at the supplier. The suppliers spend large amounts on security and have a better possibility to protect the information [GF00].

The risks that occur today have often more to do with systems going down and applications not working right, rather than someone breaking in [MD01].

Six out of ten companies in the ASP business will have closed down from the market in 2002 says a report from the Gartner Group. The report lists the main risk factors against the ASP [CS01:1]:

- The ASP suppliers cannot guarantee that company information from different customers will not be mixed. The security issue must be put in relation to the price and the security that the customers already have in their business. In Sweden the ASP suppliers offer better security than the customers can handle for a lower cost.
- The customers’ investment in the infrastructure is a high threshold for employing an ASP supplier. Many wonder “why should we change now when we already have a working IT environment?” They forget that it is not necessary to change the present infrastructure.

Security is an important reason to the customers’ hesitation. Many think that the negative experiences some customers have had will not make them more eager to getting an ASP solution [CS01:2]. To resign all responsibility for the IT-operation is a big decision.

According to the interviewed suppliers the biggest risks for the ASP company is its own customers errors. The customers present an error in the way they sometimes handle their passwords to casual or their lack of knowledge when it comes to new techniques.

The most occurring security risk is according to the suppliers the human error committed by their customers when there is a lack of correct security policy.

3.4.1 Risk management

There is nothing that is completely 100% safe. It all comes down to a question of risk management. Risk management is a process of determining exactly how much security you actually need. When deciding how much effort to spend on securing a network, the value of the data in the network, the publicity of visibility of the organisation and the harm that could be caused by loss of service, needs to be known [SP00].

To do a proper risk analysis there are a few fundamental questions you need to ask [KA01]:

- What is business process worth, and what if it stops?
- What exactly am I protecting and is it at risk?
- What are the risks involved?
- What are the different ways of lowering risks?

You also have to define what is needed by asking these questions:

- How sensitive is the data?
- Who will be using the application?
- How sensitive is the data involved in the application?
- Would anyone care if an unauthorised employee saw the data?
- Would anyone care if a competitor saw the data?

The risks that should be analysed can be seen as a combination of the probability that a threat should lead to an action and therefore unwanted consequences. The consequences can be classified as devastating, serious, mild or non-existent [LB93].

The result of a risk analysis can together with judicial conditions be used as basis for defining an information classification model for the organisation.

In all the interviewed supplier companies some kind of risk analysis exist. Often the personal is educated in the SBA-method developed by the Computer association of

Sweden. The risk analysis is used both on their own companies and their customer who have to be actively involved in it.

3.4.2 Information classification

An important activity for attaining high security is to be able to classify information to obtain correct security level. All work with information security assumes that you want to limit the risks for the possibility that the information is affected in a non-desirable way and give negative consequences [LG93].

Found labels in military security policies include top secret, secret, confidential, and unclassified. Each label presents a level of information that is more restrictive than the previous label. The labels are in a relationship to each other, stating who is higher than whom. The purpose of labelling is to prevent a user who is classified at only the confidential level from accessing information at the secret or top secret level [ET98].

You should start with identifying the risks for: poor availability, unauthorised access, lack in quality, and key persons. To identify the risks you need to apply a systematic and structured analysis work, which studies the risks in both the developing- and administrational phase of an information system.

When the groups of information are classified they should all be divided into four levels to be able to see how sensitive the information really is. When the information is classified in a manner that suits the company, you turn to classifying the system itself [LB93].

A “normal system” will work efficiently and not cause any irritations or unnecessary problems. It will not have any operational demands on it. The information in the system is open and available at all levels.

An “important system” will cause the company a noticeable economic loss if it has down time or offers wrongful information.

A “critical system” will cause the company large economic damage/losses if it has even the smallest down time or through loss of information.

The difference between the information classification and the risk analysis, is that when doing an information classification you value the information from the view of what negative consequences that will occur if something happens. No regard is taken to the fact of how probable the risk is to occur or what kind of security measures that has been taken.

The consulted suppliers feel that classification of the information totally depends of what kind of information that should be managed. The majority of them do how ever provide the possibility for their customers to classify the information if the customer internally want to separate the information.

4. Analysis of customer interviews

The analysis is divided into different chapters depending on the subject at hand. Subchapters are divided depending on which department the interviewed persons work at. This is done because of the differing knowledge basis between the departments. As we have mentioned before we have interviewed four people at the IT-department, six people at the personnel department and four regular employees.

4.1 Security

4.1.1 IT department

As the employees within the IT-department are involved with security activities, they have a broad knowledge of Internet and security. They know what is demanded and required to assure a secure network environment. In general, the employees that counted their business as some kind of ASP activity thought that they had very good knowledge of ASP, while others had only heard about it and knew the concept.

The confidence in ASP companies and the security that they provide is in general high. They know that the ASP companies have professional employees that can manage security issues. If the ASP benefits from the security that is provided by trustful sub-suppliers, such as Säpo, the confidence would definitely increase, says one of the employees.

Concerning the security of data from a third party, the ASP companies are considered to be more reliable if they use the personal integrity agreements like the Swedish Personal Register Law, the Official Secrets Legislation, and the Legislation on Swedish Computer & Privacy law.

When talking about the data security aspects, they all require that firewalls, separate networks between the ASP service and the ASP development, encryption lines between the ASP and the customers, regular backups, and agreements are necessary. All these factors should be, according to them, adapted to the customers' business environment. Some of the employees also pointed out that the security level of data should be as safe as they have in their own organisation. An inspection at the ASP companies' location is also necessary.

4.1.2 Personnel department

In comparison with the employees at the IT-department the knowledge of the concept of ASP and its meaning is reduced. What they know about ASP is what has been spoken in the media. The knowledge about Internet and its security is also mostly gained through the media. The overall feeling is that the Internet should not be considered as completely secure.

The demand on security is hard to define other than saying that it has to be safe, say the majority of the interviewed people. Some are of the opinion that if their own IT-department is satisfied, then it is sufficient for them, as well.

4.1.3 Regular employee

As with the employees at the personnel department, the regular employees have not really heard about the concept of ASP. They have no substantial knowledge about ASP at all. They have also no considerable opinions about the Internet and the security there. They use the Internet, but are not sure about how much to trust it.

When it comes to determining the security level of such a system, two of them think that they know too little to say, and the other two say that if their IT-department have checked the ASP supplier out, it is okay.

4.2 Availability

4.2.1 IT department

The opinion about the availability of the system is required to be 100%, or as much as their own company can provide (99,5-100%). But the availability demands depends also very much on what kind of system that is used. Some systems could, for example, be available between 8-20 a clock each day, while other systems need to be available 24 hours a day.

4.2.2 Personnel department

The demand on the availability of a system provided by an ASP is varying on what kind of system you are talking about. Some feel that it depends on if the system is intended for internal or external use, and for some it is related to the demands from their own IT- department. But overall the percentage that they talk about is from 99,5-100% availability.

4.2.3 Regular Employee

Their demands concerning the availability of a system is a majority towards 100% of availability.

4.3 General opinions

4.3.1 IT department

The ASP concept in whole is accepted in general, but when it comes to decide if their own company would benefit from an ASP solution, it is a question of cost and security. If the ASP can provide the same, or higher, security than they have in their company, and if it shows that it is cheaper to maintain, than an ASP solution could be an option, says one of the employees.

The disadvantages with ASP, seen from their point of view, are that they do not have any control of the system and security environment. It is also mentioned that there could be difficulties in adapting the application to the customers business. Another factor that is thought of is the priority that is given to the customers, because there is a risk that larger companies could have higher priority than smaller companies. The agreements should not be underestimated as well, as there is a possibility that disputes can occur concerning the requirements.

A signed agreement between the customer and the ASP supplier is relevant. Either it is a Server Level Agreement (SLA), Satisfaction Guarantee, an IT-business Agreement Sweden, or a self declared agreement it is very important to have something to fall back on (See APPENDIX A). In every agreement their is expected to be clearly written security aspects and the way to manage them like how to restore data, backups (which is expected to be at least once a day), availability etc.

A recruitment system is seen as a positive investment for the company, depending on how much it will cost. Some think that it would definitely be an advantage if the company could benefit from the resources that already exists within the company. It would be cheaper to employ an existing employee that already knows the company, rather than finding a person with the right competence outside, who would have to be adapted to the new business environment.

The data confidentiality and integrity in a recruitment system is important. None of them would like it if the data about who is looking for what job, who is recruited and other personal data was displayed for everybody. This could be measured with the fact that the security is expected to be as high as a banking system, which in general is seen as one of the securest systems that exists.

4.3.2 Personnel department

When it comes to trusting a system for storing information, that is reachable from the Internet, compared to having the system in-house, the feelings are divided fifty-fifty. Half feels the insecurity when dealing with Internet and half feels that if there is a sufficient agreement with the ASP there should not be any problem in trusting them, even if having a system in-house could increase the feeling of pleasantry. For more information about the different agreements, see APPENDIX A.

The trust for the ASP suppliers is something that depends largely from case to case. A supplier is always a supplier and the feeling of not having control over ones data is present. Since the opinion is that the Internet is insecure, the security at the ASP suppliers can neither be trusted completely.

When comparing their own IT-department to the ASP, the trust mostly lies with their own IT-department. This due to the fact that with their own IT-department they know what they have and what they will get. One person thinks that as long as the demands are met and the agreement is followed, there is no difference between hiring a system from an ASP or having it within their own company.

About the advantages concerning the ASP the answers are that they mostly do not know enough about it to make any statements. However one of the interviewed thinks that the advantages of using ASP depends on the size of the company. One person thinks that another advantage is that an ASP solution would be fairly easy to use comparing to a normal system.

One of the disadvantages is stated to be the fact that you feel loss of control, when the system is not “in” the company. Also the belief that it is hard to live up to the security demands, is one disadvantage according to one person. Otherwise the answers here agrees with the ones given about advantages, they do not know enough to make an opinion.

The idea of an internal recruitment system is generally well received, and two of the companies already have a solution for internal recruitment. For the municipality the solution would not be a good solution, since the publicity laws is applied on their data. However, there is an interest for it anyway. When talking about who should be qualified to use an internal recruitment system, the opinion is that it should be controlled with different access levels.

A system for Internal recruitment should have a security level that is comparable to a banking system, since personal information is very important and there are laws regulating the handle of that kind of information. Only one of the companies, since they are a municipality, has to have official recruitment stages.

4.3.3 Regular Employee

When it comes to their trust towards an ASP supplier three fourths of them states that they do not have much trust for the ASP and leaving information to a third party feels insecure. The last one feels that he can trust an ASP supplier and that they are secure.

If comparing the ASP suppliers to their own IT-department the feeling of trust is fifty-fifty. Two persons think that it would be more secure to have the system in-house and two persons think that it does not make a difference.

When talking about if there is any difference in trusting a computer system to store information compared to a company that have the information in paper, again hackers are a big reason for not trusting the computerised system, but a majority trusts the computer system more. One person mentions though that it is rather silly and not very logical, to see any difference between the two.

The advantage with ASP they mention is the fact of being excused from doing all the administration. They all feel that they know to little about ASP to say much more.

A disadvantage that is pointed out is that you might feel too independent when someone else has the control of the data.

All of them can consider storing their personal information in a system that can be reached from the Internet. If they want to do it is another question. When storing information that can be reached from the Internet, their biggest fear concerns hackers and others persons possibility to access the information illegally.

The idea of a recruitment system within the company is also here an accepted idea. One of the employees states that her company already has such a solution, which works satisfactory. The security level of an internal recruitment system should be at least as high as a banking system.

4.4 Level of interest

When looking at the level of interest we have to look at two different areas: the interest for ASP and the interest for the internal recruitment solution. The interest is measured with three categories:

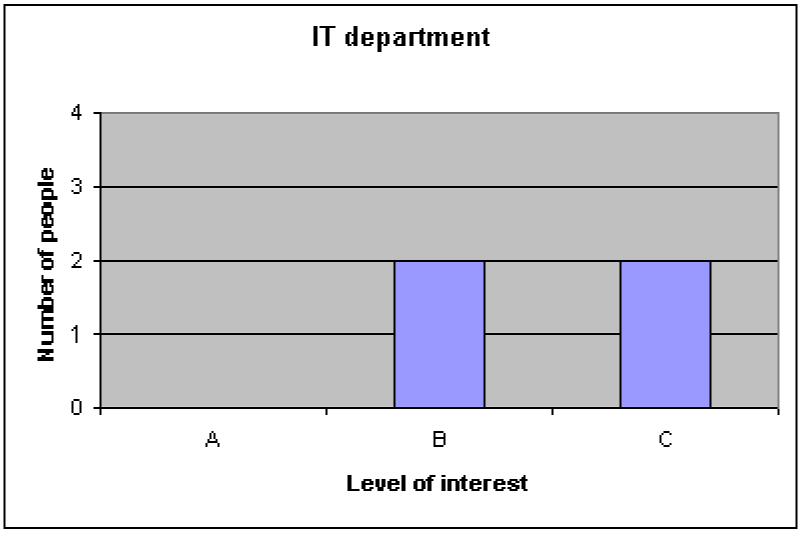
- A = Interested, and want to test it.
- B = Interested, but want more information.
- C = Not interested.

A and B are considered as a positive reaction to the relevant question, where as C is considered to be negative. The written interpretation of the graphs will be presented in the next chapter, 5. Result.

4.4.1 ASP solution

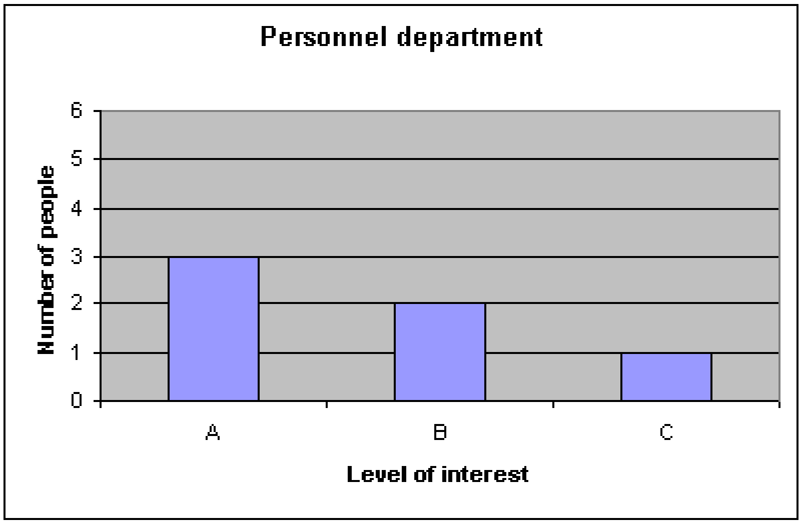
When looking at the interviewed customer’s interest in any kind of ASP solution, not specifically the internal recruitment solution, we have found out that:

The people at the IT department are divided in this manner:



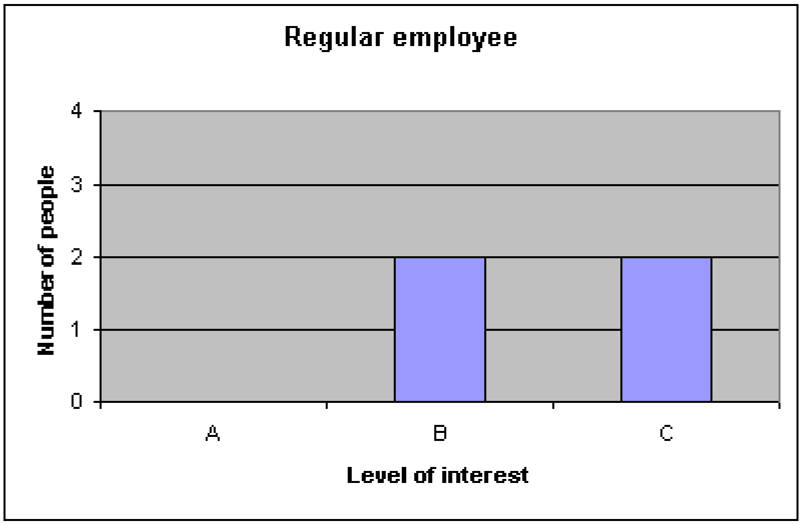
Graph 4.1 The level of interest for ASP within the IT department

The people at the personnel department are divided in this manner:



Graph 4.2 The level of interest for ASP within the Personnel department

The regular employees are divided in this manner:

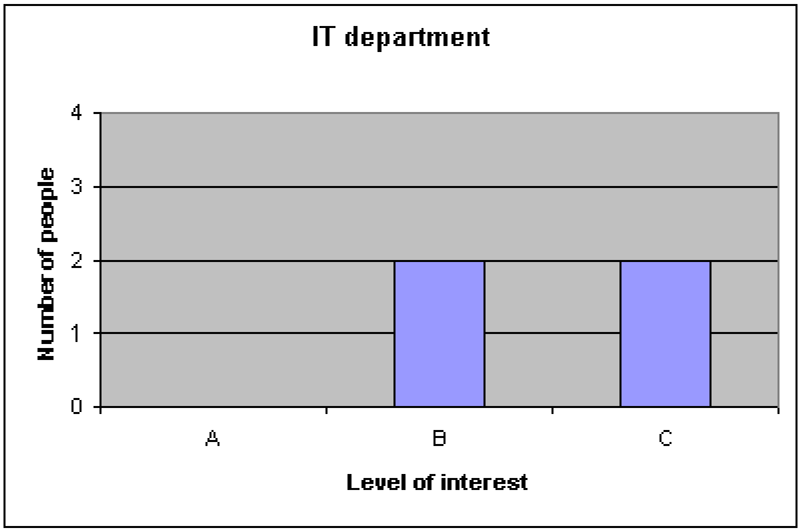


Graph 4.3 The level of interest for ASP among the Regular employees

4.4.2 Internal recruitment solution

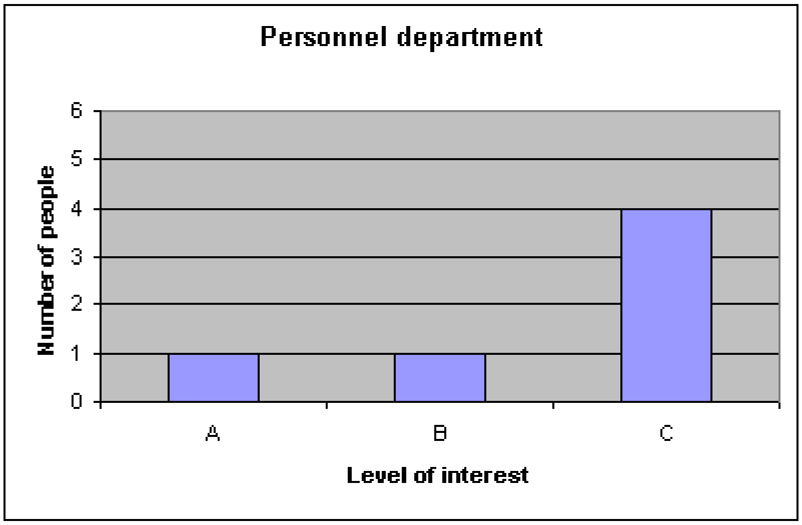
When looking at the internal recruitment solution the interest is as follows:

The people at the IT department are divided in this manner:



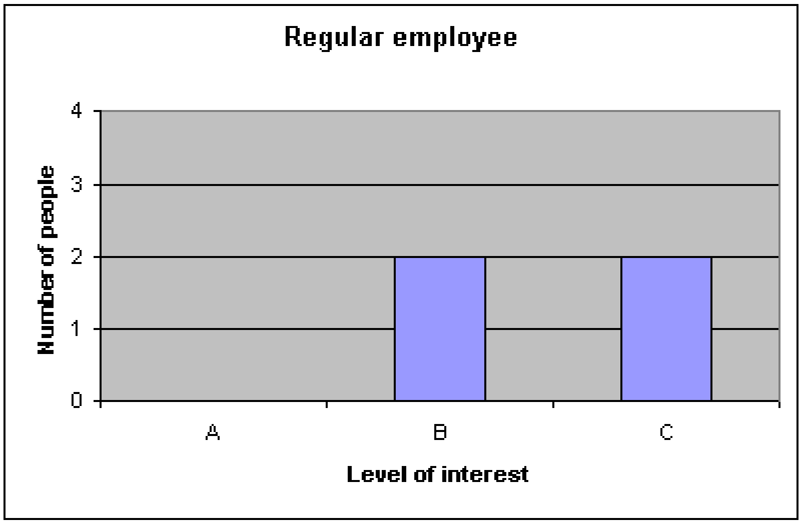
Graph 4.4 The level of interest for the Internal Recruitment system within the IT department

The people at the personnel department are divided in this manner:



Graph 4.5 The level of interest for the Internal Recruitment system within the Personnel department

The regular employees are divided in this manner:



Graph 4.5 The level of interest for the Internal Recruitment system among the Regular employees

5. Result

5.1 Hypothesis

"Companies are willing to consider an ASP-solution if certain demands are met. This includes demands on security and availability."

In the end of this investigation, we have realised that we cannot estimate and apply a result for a whole company. The result considering an ASP-solution is therefore determined for each department.

Two out of four people, from the IT departments, have a positive attitude and can consider an ASP solution, while the rest are not interested.

Five out of six people, from the personnel departments, have a positive attitude and can consider an ASP solution, while the last one is not interested.

Two out of four people, among the regular employees, have a positive attitude and can consider an ASP solution, while the rest are not interested.

Looking at all the departments together, a majority (9 out of 14) can consider an ASP-solution, while the rest are not interested.

As the hypothesis is stated above we cannot verify it, but if dividing the companies into their departments the hypothesis is proved.

5.2 Research questions

- *Is ASP reliable concerning storage of information?*

The data storage aspects that serious ASP suppliers provide is reliable, since they use methods that are protecting the data from physical, external, internal and personnel related damages. Most of the suppliers store the customers' data on separate logical databases within a shared physical web server, where the physical resources are protected by using co-location facilities. This is the most secure way for serious ASPs to protect their customers' data.

-*What is expected from an ASP-solution to be trusted by customers?*

To trust the ASP, a written agreement that is followed by the suppliers is necessary. The ASP must provide confidentiality, integrity and availability of data in accordance to the customers' requirements of security level. The lack of criminal records of the employees at the ASP should also be inspected, so the customers know that the suppliers can provide trustworthy staff.

- *How can the security level within an ASP-solution be determined for the customers?*

The ASP customers and suppliers determine the security level by classifying the customer's data and by doing a risk analysis.

6. Discussion

6.1 Conclusion

The ASP industry is clearly in the stage of maturity within the IT business. As the concept is a new way of looking at the possibilities of making business through the use of Internet, it increases also the worry of letting a third party take care of company data.

ASPs should, however, be considered as a business that has data reliability, security and availability as their profession. They work with advanced systems infrastructures and up-to-date technology in trying to give the customers the best service possible. If the ASPs do not succeed within these areas, this will ruin their reputation and the customers' trust.

In order to effectively ensure reliability, availability and security, ASPs will need to invest in spare capacity, in system management and modelling tools, and advanced security tools. None of this is cheap, and ultimately only those ASPs winning sufficient business will be able to afford to put the necessary infrastructure in place.

Customers who turn to ASPs often find better application reliability and availability than they experienced from their internal IT organisations. Often the security level is higher at the ASP than the customers. As we have stated before, the reason for this is that running information systems for other entities is the ASP's primary business.

However, even though an ASP solution seems to be a successful approach, there a tangible threats in today's reality.

The immaturity within many ASP businesses harms the reputation for the others.

Customers that decide to run ASP solutions do not completely understand what they want. This causes conflicts later on when the customer realises that the agreement that was signed was not really what was expected or wanted.

In the end it seems like the psychological barrier may be the strongest one that can diminish the success of ASP.

"The future of system usage is not set. ASP solutions may or may not have a bright future, depending on the user climate and other factors, the most important one being trust.

If trust between the suppliers and the customers is achieved and maintained the ASP solution can flourish as a concept" (ASP supplier).

6.2Validation, reliability

The method of collecting materials from text and interviews is, according to us, the proper way to get a result for our hypothesis. Reflecting the theories with both written material and interviews shows the reality.

When looking back, we realise that certain elements within the interviews could have been done differently to obtain even better results.

- We would probably have got more information out of the interviews, if we had interviewed all the customers personally.

- The fact that all the companies regarded as customers are large, and have an IT-department, may have affected the level of interest in an ASP solution in a negative way. Theories have shown that companies with their own IT-department do not always see the need of an ASP solution, as they think that they can provide the same service within the company.

Even though, these elements exist, we do not think that they have effected the result in such a way that it would have changed from positive to negative. We consider the result to be reliable.

6.3 Future research

Interesting areas for further research could be:

- Security policies within the ASP companies
- Physical security
- The impact of agreements
- Comparing the security level between the customers, that has an IT-department, and the ASPs.
- Digital signatures

7. Reference literature

7.1 Books:

[SE00] ASP – Application Service Providing, SCN Education B.V, Vieweg & Sons, 2000 ISBN: 3-528-03148-4

[LG93]Att klassificera information- Ett debatt inlägg, Ledell G. Dataföreningen i Sverige, 1993 ISBN: 91-86656-57-0

[LB93] Client/server och Säkerhet, Lindberg B. SIG Security, 1993 ISBN: 91-86656-68-6

[SP00] Firewalls 24seven, Strebe M, Perkins C, Network Press, 2000 ISBN: 0-7821-2529-8

[ET98] Intrusion Detection, Escamilla T, Wiley Computer Publishing, 1998 ISBN: 0-471-29000-9

[GS97] Web Security and Commerce, Garfinkel S. Spafford G. O'Reilly, 1997 ISBN: 1-56592-269-7

7.2 Exam thesises:

[KP96] Informationssäkerhet i lokala nätverk, Kirsten P, Exam thesis ADP-C, BTH, 1996

[GF00] Uthyrning av IT-tjänster via Internet, Glennsjö F, Exam thesis economy, LiTH, 2000

7.3 Articles:

[KA01] ASP planning: A checklist for Security, Kelman A. e-Business Magazine, 1 March 2001

[MM00] Don't overlook security in ASP selection, Martin M. Network World, September 18, 2000

[LB00] I framtiden hyr du programmen via webben, Larsson B, Nätverk & kommunikation No. 5 2000

[ÅB01] Internetberoendet ett orosmoln för programuthyrning, Åslund B. Computer Sweden, 21 March 2001

[CS01:1] Kritiken mot asp skjuter bredvid målet, Computer Sweden, 2001

[SH00]Tekniken bakom ASP: så går det till när du hyr applikationer på nätet, Skalin H. EVärlden, No:4 2000

[MD01]The ASP solution: Stop!Thief!, McWhirter D. CRM, January 2001

[JLR01] Varför allt fler e-hostar, Johansson L.R, Computer Sweden, 2001, Appendix from IBM and Partners

[CS01:2] Utslagning väntas bland asp-företag, Computer Sweden, 2001-03-23

7.4 Internet pages:

[ECE01] ExpoNova Calender of Events 2001, May 8, 2001
http://www.exponova.se
[SC01] ServCentric, http://www.servcentric.com/what_asp.html, 2001-05-13
[SM01] The Elements of the ASP Market, Sun Microsystems. 2001-05-14
http://www.sun.com/software/solutions/thirdparty/hosting/pdf/InfrastructureWP_GD_8=21.pdf
[JOB01] Jobado AB, http://www.jobado.se , 2001

8. Other literature

8.1 Books:

- Brandväggar vid anslutning till Internet, Statskontoret, 1995
  ISBN: 91-7220-248-3
- Forskningsmetodikens grunder, Patel R, Davidsson B, Lund Studentlitteratur, 1994
- Internet and intranet security, Oppliger R, Artech House Boston, 1998
  ISBN: 0-89006-829-1

8.2 Exam thesises:

- Analys av datasäkerheten – i och omkring patientjournalsystemet i Varberg, Andersson L, Andersson M, Exam thesis ADP-C, BTH, 1995
- Internet - Något för ett företag, Arvidsson H, Eriksson J, Lundgren T, Exam thesis ADP-C, BTH, 1995

8.3 Articles:

- A Ess Pé – va’ é dé?, Skalin H. eVärlden, No 4 2000
- ASP en tom marknad som alla tror på, Åkerman C. Datateknik 3.0, No.7 1999
- ASP enda alternativet för Blåkläder, Nordling E. Datateknik 3.0, No: 13 2000
- ASP: service byrå med Windows stil, Sigurdson O, Datateknik 3.0, No. 13 2000
- För mycket teknik hämmar säkerheten, Computer Sweden, 2001-04-06
- How to decide weather to outsourcing is for you, Blum D. Network World, January 2001
- Inhyrd brandvägg över nätet, Widman M. eVärlden, No: 4 2000
- IT-företagens avtal: kort presentation, Svenska IT-företagens organisation, 2001
- Kan du lita på ASP?, Åkerman C. Datateknik 3.0, No: 7 2000
- Moderna Protokoll är ett måste för ASP, Dahlin N. Datateknik 3.0, No: 13 2000
- Nätets tjänstefolk, Affärsvärlden, No: 11 2000
- SLA picture clearing up for ASP users, Mears J. Network World, January 2001
- The outsider, Dunn S, Searchbusiness.com, No: 18 2000

8.4 Internet pages:

- Application Service provider, What’s?com, January 19, 2001
  http://whatis.techtarget.com
- Writers Handbook (IMRAD), The Writing Center, February, 2001
  http://www.wisc.edu/writing/Handbook/ScienceReport.html

9. Wordlist and Abbreviations

Co-location facility = a business for renting fully secured and maintained server location.

Swedish Personal Register Law = a law that regulates the publication of information about individual persons on the Internet.

Official Secrets Legislation = a law that regulates confidentiality and the distribution of personal information.

Legislation on Swedish Computer & Privacy law = a law that regulates the permission for the, so called, personal register to protect individual integrity from unauthorised access.

Cryptography = the science of enabling secure electronic communications between a sender and one or more recipients.

APPENDIX A

Agreements

The problem for most customers is that they do not know what to ask for when it comes to the ASP supplier. To help trust the supplier a written agreement between the customers and suppliers can be of help. An agreement is also a help for the ASP suppliers to define actually what service level they can guarantee. With the agreement you can put down rules for any kind of situation involving the provided service from the ASP supplier. They can address response time, disasters, recovery, and storage utilisation.

There are four kinds of agreements that are in use today: the SLA, Satisfaction Guarantee, IT-business agreement Sweden, and an own written agreement. The last one is not any kind of standard but an agreement assembled between each customer and the supplier. Here follows a short description of the other three.

SLA

A specified Service-Level Agreement (SLA) is defined for each customer. These agreements provide contractual assurance that a given level of availability, response time, or business service accessibility will be met. They follow the standard provided by the ITTA – Information Technology of America. They are written with facts and numbers to what needs to be followed.

Satisfaction Guarantee

A satisfaction guarantee is a contract or document mostly just stating that if the service is to a satisfactory state to the customer the agreement is fulfilled.

IT-business agreement Sweden

This is a new kind of standard agreement directed at the market in Sweden. There are especially two standard by the names: IT-operation and agreement 90 that are directed at the ASP business. With a standard agreement the customer can compare different suppliers offers to each other.

This information is taken from the articles:

- SLA picture clearing up for ASP users, Mears J. Network World, January 2001
- IT-företagens avtal: kort presentation, Svenska IT-företagens organisation, 2001

APPENDIX B

Interview questions for ASP suppliers

GENERAL

1. How do you define an ASP solution?
2. Does ASP solutions fit in all kinds of usage areas? For ex. Word-processing, mail programs, and drawing programs.
3. What controls the availability of the ASP solution?
4. How big percentage of availability do you guarantee? Do the customers have reasonable demands on the availability?
5. Do you have some sort of SLA (Service Level Agreement) with your customers? Have you followed the standard of the ITTA?
6. What is generally the Achilles' heel of the ASP suppliers?
7. What do you consider being the biggest threat to your organisation?

DESIGN

8. What would you consider being the ultimate system security architecture? I.e. Firewalls, separate network, and so on.
9. How do you classify information that shall lie in the system?
10. How do you separate the different customers' data? Do you separate it both physically and logically or one or the other?
11. How controlled is the physical access to your servers?
12. Do you have any reserve lines for your Internet access?

SECURITY

13. Where lie the risks within the security for an ASP solution?
14. What is the most usually occurring security risk?
15. Are there any obvious security levels? If so what?
16. In what manner are these security levels classified?
17. Does different customers have different security levels? Why is it so?
18. Does the ASP suppliers have any security standard? Is there one official standard?
19. Is there any maximum of minimum level for how many security measures that should be taken?
20. What kind of security does the customers generally have when you come in with your solution?
21. Have you noticed any difference in the security at ASP suppliers related to the size of the suppliers company?
22. What is according to you the positive with firewalls? Why do you use them?
23. How often is backup done on the data?
24. What kind of backup is mostly used? The most secure?
25. In what way do you secure the data from being altered or destroyed?

26. How can the data be altered or destroyed? What can be the reason? How fast can it be restored?
27. Do you have any kind of intrusion detection? What can you do to prevent intrusions?
28. What kind of virus protection do you have?
29. What do you think about SSL (Secure Sockets Layer)?

ABOUT THE CUSTOMER

30. What are the advantages with ASP? For the supplier? For the customer?
31. Do you feel that the customers trust you or do they show worries?
32. What do the customers perceive as insecure?
33. How do you handle customers’ insecurity?
34. Do you conduct risk analysis? If so how? Do the customers take an active part?

APPENDIX C

Interview questions to customers

IT-DEPARTMENT

1. Have you heard about ASP - Application Service Provider?
2. Do you know what ASP involves?
    - How much do you know about ASP?
3. What do you know about Internet and its security?
4. How much do you trust on the data security at an ASP supplier?
5. What kind of demands on the availability do you have on a system?
6. Do you think that an internal recruitment system should have a higher security level than a banking system? How high do you value your personal information? (Observe that account numbers is not counted)
7. What would you think about an Internal recruitment system within you company?
8. What kind of security demands would you have on the recruitment system and the ASP supplier?
9. Can you see any advantage with ASP?
10. What kind of disadvantages can you see with ASP?
11. How often do you think backups should be taken on the information?
12. What kind of backup do you demand?
13. Would you demand a written SLA (Service Level Agreement) or is a “Satisfaction Guarantee” enough?
14. What would you consider to be the ultimate security architecture? I.e. Firewalls, Separate networks A. S. O.
15. What would you consider to be the minimum level of security to protect the information in the system?
16. What kind of security levels do you have on your own systems in the organisation today?
17. If an ASP solution fulfils your demands, would you have any interest in it then? Specify your answers by selecting one of the following alternatives:
    a) Interested, and want to test it.
    b) Interested, but want more information.
    c) Not interested.

18. If the Internal recruitment system fulfils your demands, would you have any interest in it then? Specify your answers by selecting one of the following alternatives:

    a) Interested, and want to test it.
    b) Interested, but want more information.
    c) Not interested.

PERSONNEL DEPARTMENT

1. Have you heard about ASP - Application Service Provider?
2. Do you know what ASP involves?
    - How much do you know about ASP?
3. What do you know about Internet and its security?
4. How much do you trust on the data security at an ASP supplier?

5 What kind of demands on the availability do you have on a system?

6. Do you think that an internal recruitment system should have a higher security level than a banking system? How high do you value your personal information? (Observe that account numbers is not counted)
7. What would you think about an Internal recruitment system within you company?
8. What kind of security demands would you have on the recruitment system and the ASP supplier?
9. Can you see any advantage with ASP?
10. What kind of disadvantages can you see with ASP?
11. Companies put a lot of money into recruiting persons with the right competence. What they often don’t know is that with an internal recruitment system you can search for already employed people with the right competence and there by recruiting them more economical. How would you feel about such a solution for recruiting?
12. Do you see any difference in trust in storing your information in a system that can be reached from the Internet compared to storing it at a company, for ex. A revision bureau?
13. Would you trust more at you own IT-department than in an ASP supplier? In other words would it be more comfortable to store the information in a system that is administrated and supported within you own company than with an ASP supplier? If so then why?
14. What kind of information would you want the employees to store to benefit the internal recruitment process?
15. Who should have the authority to use the system for recruiting?
16. If an ASP solution fulfils your demands, would you have any interest in it then? Specify your answers by selecting one of the following alternatives:
    a) Interested, and want to test it.
    b) Interested, but want more information.
    c) Not interested.
17. If the Internal recruitment system fulfils your demands, would you have any interest in it then? Specify your answers by selecting one of the following alternatives:
    a) Interested, and want to test it.
    b) Interested, but want more information.
    c) Not interested.

REGULAR EMPLOYEE

1. Have you heard about ASP - Application Service Provider?
2. Do you know what ASP involves?
   - How much do you know about ASP?
3. What do you know about Internet and its security?
4. How much do you trust on the data security at an ASP supplier?
5. Could you consider storing your personal information in a system that can be reach through the Internet?
6. What would worry you the most if you had information like your CV, experience report, and such stored in such a system?

6 What kind of demands on the availability do you have on a system?

7. Do you think that an internal recruitment system should have a higher security level than a banking system? How high do you value your personal information? (Observe that account numbers is not counted)
8. What would you think about an Internal recruitment system within you company?
9. What kind of security demands would you have on the recruitment system and the ASP supplier?
10. Can you see any advantage with ASP?
11. What kind of disadvantages can you see with ASP?
12. Do you see any difference in trust in storing your information in a system that can be reached from the Internet compared to storing it at a company, for ex. A revision bureau?
13. Would you trust more at you own IT-department than in an ASP supplier? In other words would it be more comfortable to store the information in a system that is administrated and supported within you own company than with an ASP supplier? If so then why?
14. If an ASP solution fulfils your demands, would you have any interest in it then? Specify your answers by selecting one of the following alternatives:
    a) Interested, and want to test it.
    b) Interested, but want more information.
    c) Not interested.
15. If the Internal recruitment system fulfils your demands, would you have any interest in it then? Specify your answers by selecting one of the following alternatives:
    a) Interested, and want to test it.
    b) Interested, but want more information.
    c) Not interested.