BUSINESS INTELLIGENCE AND INFORMATION WARFARE ON THE INTERNET

Mikael SIMOVITS

ICL SVENSKA AB
Torshamnsgatan 36 - 164 93 Kista - Suède

Tomas FORSBERG
ABB INFOSYSTEMS AB
Stora Gatan 3 - 721 80 Västerås - Suède

BUSINESS INTELLIGENCE AND INFORMATION WARFARE ON THE INTERNET

Mikael SIMOVITS

ICL SVENSKA AB
Torshamnsgatan 36 - 164 93 Kista - Sweden

Tomas FORSBERG

ABB INFOSYSTEMS AB
Stora Gatan 3 - 721 80 Västerås - Sweden

Business Intelligence (BI) and Information Warfare (IW) on the Internet is today a reality and in many ways a growing problem. Data Security is no longer a matter of preventing intrusions. Information on the Internet can in many ways cause a company or organisation considerable damage. Even if old rules regarding classification of information are kept, the new concentration and availability of information makes it vulnerable. This article discusses methods used by companies and organisations to both reach and spread information on the Internet. The problems, methods and techniques are described, and placed on an ethical scale. The cases and methods mentioned in this article are based on actual events on the Internet. These problems, and their immediate and long-term consequences, will also be discussed together with corporate views on information security. Special consideration has been given to the searching engines and index servers on the Internet. Together with other methods, these services provide new and unique opportunities to both find information and to trace its usage.

Introduction

Data Security is today an inexact science and it is difficult to define what security is all about[1]. It is also difficult to define the threats since it is almost impossible to detect, track and catch an intruder. Some attempts have been made to quantify the threats. In May 1996, GAO (General Accounting Office, USA) released a report on the security of the systems belonging to DoD (Department of Defence) connected to the Internet. The report described a test where an attack was made on 38,000 of their own systems. Two thirds of the attacks succeeded. In only 988 cases were the attempts detected, but only 267 of those were reported[2]. In many cases intrusions are believed to be the only threat from the Internet, which in many cases may cause the community to believe that Data Security can be measured with two fixed states, e.g. that Data Security/Computer Security is binary. The Internet has given new opportunities to "steal" information, but it has also given an unlimited number of ways to manipulate, market and gain information without breaking into or damaging systems. This article is focused on the problems related to Data Security, and since the Internet is regarded as a global network without international boundaries this puts BI and IW in a new light. This phenomenon has been observed in several articles, but has not been described in a clear and technical way. This article is divided into three parts. Part one describes the taxonomy around Business Intelligence and Information Warfare, and old values concerning these subjects. The second part will describe how Business Intelligence is used on the Internet. Part three will describe how Information Warfare is used on the Internet. The problems concerning BI and IW will not only be presented but also put into an ethical scale.

Business Intelligence and Information Warfare

The way a company, in one country, acts toward a competitor is determined by that company's and that country's ethical values. An action may be regarded as "industrial espionage" or "terrorism" in one country, while in other countries the same action may be regarded as a common way to gain information or gain market share. Industrial espionage falls under the collective term "Business Intelligence". Business Intelligence is defined as an activity to overview the external environment of a company, with the intention of finding information that can be incorporated in the management process of the company[3]. Some state that BI does not incorporate any illegal activities, and that it is a passive method of getting information. It is difficult to draw a line between "Business Intelligence" and what is regarded as illegal industrial espionage[4]. The law and ethical values decide where the line is drawn regarding retrieval and use of information. The following table is a graduation of the means a company might use to get information about competing companies[5]:

1. Published material, and public documents such as court records.
2. Disclosures made by competitors' employees, and obtained without subterfuge.
3. Market surveys and consultants' reports.
4. Financial reports, and brokers' research surveys.
5. Trade fairs, exhibits, and competitors' brochures.
6. Analysis of competitors' products.
7. Reports of salesmen and purchasing agents.
8. Legitimate employment interviews with people who worked for competitor.
9. Camouflaged questioning and 'drawing out' of competitors' employees at technical meetings.
10. Direct observation under secret conditions.
11. False job interviews with competitors' employees (i.e. where there is no real intent to hire).
12. False negotiations with competitor for license.

13.Hiring professional investigators to obtain a specific piece of information.
14.Hiring an employee away from the competitor, to get specific know-how.
15.Trespassing on competitors' property.
16.Bribing competitors' supplier or employee.
17.'Planting' your agent on competitors' payroll.
18.Eavesdropping on competitors (e.g. via wire-tapping)
19.Theft of drawings, samples, documents and similar property.
20.Blackmail and extortion.

This list was published in 1966 by Dr. Worth Wade, and is referred to as "The Wade System of Graduation of Sources of Information." The first seven methods are usually ethical and legal; the remaining thirteen are in a descending order of ethics or legality. It is important to notice that in some countries the entire list is regarded as a usual means of gaining information.

Information warfare on the other hand is regarded as knowingly spreading accurate or inaccurate information about a competitor or organisation, or preventing a competitor or organisation spreading its information. The information in itself is not important in this field, but what is more important is how the information is presented, where it is presented and who is presenting the information. Before the Internet, it was easy to detect moves from competitors or organisations, and it was easy to trace the information back to the source.

Business Intelligence on the Internet

BI has today an entirely new context, thanks to the Internet and other global networks. The means of collecting information was greatly simplified when international boundaries were erased and when companies themselves did not respect their own information. Above all, there are no existing laws working against "dubious" activities on the Internet. The following table is structured in the same way as the Wade graduation, describing activities observed on the Internet:

1. Periodically downloading of public WWW-servers (World Wide Web) and public file archives belonging to the competitor.
2. Collecting open information available, such as articles and news.
3. Analysing additional information available about readers of your own web site
4. Map a company by finding its partners, vendors and customers by searching for WWW-pages with 'links' to the competitor.
5. Eavesdrop and filter the information flow in USENET news and mailing lists.
6. Open analysis of a competitor's network and its users by examining information issued by electronic look-up services.
7. Map the users of a competitor. Get information about the users and their interests on the Internet.
8. Get access to a competitor's internal WWW-pages etc. with a false identity or an identity used by the competitor's customers.
9. Map a competitor's internal network in connection with projects or consultancy.
10.Intrusion.

Points 1-3 can be regarded as normal BI-activities. Points 4-6 is a more aggressive stance, which in certain conditions can be questioned from a moral and ethical point of view. Points 7-9 are directly questionable and point 10 includes only illegal activities. These methods have all been observed on the Internet, though it is still unusual for companies to use the less ethical of the methods described above.

A deeper analysis of the BI points

1. Periodical downloading of public WWW-servers (World Wide Web) and public file archives belonging to the competitor.

During the time a market reaches the levels of saturation, more and more of a company's attention is directed towards protecting its shares or more accurately trying to gain market share from competitors. It is therefore important that trends, customers and competitors' activities are monitored. It may also be of some interest to observe organisations working for the benefit of consumers, the environment and other similar fields.

The Internet is a new way for a company to spread information about its projects, services and products. Companies also use the Internet for presenting joint-venture projects, scientific reports, reviews, etc. Normally old rules regarding classification of information are not neglected, but the concentration of information and its availability makes it vulnerable.

From a technical standpoint there are several levels of ambition. The simplest solution for collecting information is to use cache-servers and to set up the necessary parameters regarding the company in question. The term "cache" describes the ability to keep collected information for a shorter time locally, in case this information is requested again. This solution can be configured to be transparent to the organisation. It is also possible to ignore settings - some companies configure their documents so they won't be cached by the documents' "expire" variable. By ignoring this variable it is possible for the organisation to have access to the information and decrease the number of visible requests made to the competitor's public servers.

At the next level, a company's machines are mirrored. A standard crawler, a search-robot, requests a home page and from there follows the document's links to other pages. When a site is mirrored in a more aggressive way, the crawler tries to get all available files on the server. Assume that a company's home page has the following URL http://www.foo.com and a link in this document leads to another document http://www.foo.com/product1/description.html. In this case the crawler also tries to get the document http://www.foo.com/product1 which, for example, can be a pointer to an index file, and also to download the file http:/www.foo.com/product1/ which, depending on the WWW-server's configuration, can give complete information about the contents of this file-directory.

A third level would include the crawler searching for certain index-files for files that describe the WWW-server. Many of these files are intended for crawlers. The simplest way to learn the names and function of these files is to study the crawlers available on the Internet.

It is also possible to use crawlers for mirroring gopher and FTP-services, to gain additional information and to see if it is possible to extract more information from the WWW-servers file-directory.

2. Collecting openly available information, such as articles and news.

One simple way to monitor the activities of a company is by searching through archives and newspapers' home pages for keywords that are connected to the company being monitored. The technology implemented is the same as mentioned in the earlier point, with the difference that only information that matches the keywords or the criteria is mirrored to your server. The term

newspaper archives also includes journals, research papers, company-related publications and local publications. Many publications from companies give very detailed information about what the company has sold, bought or what kind of joint-ventures the company has started with other companies.

If a company does not want to mirror the information itself, it is possible to buy the information from an existing information provider, either a traditional provider of media coverage or from an Internet Service Provider that provides Internet search services. In the second case the company buys certain keywords, or the entire database so that they can filter it themselves.

3. Analysing additional information available about readers of your own web site

In addition to presenting information in web pages it is possible to register all users reading the information and gathering all types of information. This information includes where the users come from, how much time they spent in each web page, which pages they followed and perhaps most important of all - which link directed them to the company's web presentation. This field "http-referer" (the word referrer is misspelled in the standard) is however seldom written to logfiles, its main purpose is to detect broken links and inform others that the page has moved. For both BI and IW purposes this is useful information which makes it possible to alter pages linked by other sites or to find sites related to their own products.

Note from RFC2068 [6]: "Because the source of a link may be private information or may reveal an otherwise private information source, it is strongly recommended that the user be able to select whether or not the Referer field is sent. For example, a browser client could have a toggle switch for browsing openly/anonymously, which would respectively enable/disable the sending of Referer and From information."

In addition to the http-referer field, additional information may be sent giving browser type and version together with the e-mail address of the actual user, and the fields displaying information about the client named From, Host, Referer and User-agent.

4. Map a company by finding its partners, vendors and customers by searching for WWW-pages with 'links' to the competitor.

Apart from knowing the infrastructure of a company it is also interesting for a competitor to map the customers, partners and joint-venture projects of a company. The public presentations of a company often include links to its customers and its partners. It is therefore possible to make a simple "reverse" search where the links for a company are searched, i.e., that a crawler is given the instructions to search for presentations that contain the string "http://www.foo.com". Normally this search string is found in documents that exist outside the targeted company's own WWW-servers and control.

It is important to understand the crawlers and search-tools correctly as their capacity has increased dramatically during the last few years. The functions that are still underdeveloped are the means to omit hits from the same directory, restrict the search geographically and restrict the language used, and more importantly, have the means to save a search for additional searches and analysis.

It is also important that the web crawlers search all kinds of text, i.e. documents, internal comments and requests for different scripts. It is even possible to search for WWW-servers containing cgi-bin vulnerabilities for the purpose of attacking these servers at a later stage.

5. Eavesdrop and filter the information flow in USENET news and mailing lists

Newsgroups, also known as USENET News, have gained new recognition and cannot be compared with previous methods for exchanging information. For every area of interest there is at least one newsgroup where those interested can exchange information. Many employees use this way of communication to discuss and solve different problems. An average company has today access to at least 2000-3000 different newsgroups and every group has an average of 50-100 posted news items every day. In other words, the news system handles a great amount of information which is difficult to monitor.

If a company, for example, wants to monitor a competitor with the domain name company.com, this company can in its own news server, filter all articles that contain company.com in the header and store these articles in its own databases. In this way it is possible to learn about the competitor's problems, competence and ongoing projects. Many employees also use their access to newsgroups for private matters – this information can also be used.

6. Open analysis of a competitors network and its users by examining information issued by electronic look-up services.

When a salesman gets a new account, i.e. is responsible for sales to a certain company, his or her first goal is to get the internal phonebook, in order to understand the company's organisation. An internal phonebook contains information about personnel placement in an organisation and their responsibilities. A salesman can, when a person within this company requests information or products, estimate his own "presale", the seriousness of the request and if he needs assistance from his own company to promote the presale process. For a salesman to have the internal phonebooks belonging to competitors is even better. It is possible from these to judge the threats from competitors and if it is necessary to make strategic alliances with subcontractors to strengthen his own position.

The electronic version of an internal phonebook is the directory-services over e-mail addresses, X-400 directories and similar information. These directory services are commonly open to simplify the communication between the company and its customers and its subcontractors. The computer network's domain-structure might also be examined. There are publicly available software which simplify the examination[7].

- nslookup - gives a simple interactive access to a DNS-server (Domain Name Service)
- dig - "Domain Internet Grouper", is a program that has many similarities to nslookup.
- doc - "Domain Obscenity Control", is a script that uses dig, looking for and finding failures in the configuration of a DNS-structure.
- host - is not as advanced in its function as nslookup and dig, but is enough for getting information from a DNS-server.

If a company's inner network is open towards the Internet on an ICMP-level (Internet Control Message Protocol), is it possible for a person from the outside with traceroute and similar functions to estimate the number of addresses in use and how these addresses are segmented in different subnets. The subnet segmentation can give indications about what kind of computer systems are in use in different buildings. This information can be used together with the information gained from the DNS-server and mail-servers, and can give a much clearer picture of the network and the organisation within that company.

7. Map the users of a competitor. Get information about the users and their interests on the Internet.

As the Internet is becoming more and more commercialised, there is an increasing need for gathering statistics over the use of different resources. This is particularly important for WWW-hotels, i.e. when a company is financing the equipment and support to allow different companies to rent a place for their own presentation. It is now becoming more usual that these are also financed by selling commercial space on popular WWW-pages. The price is different for different pages. A page that is very popular is often more expensive to advertise on. This has led to the development of certain tools that give statistics on how popular certain pages are. It is today possible to track a user's browsing activities in a server, and even to know which link the user followed to get out from the server. This information can be filtered on a personal basis, for accounting purposes or to see which page is the most popular. Today this function is more or less regarded as state of the art, but the tendency is clear.

What is terrifying from a BI-perspective is that this information can be used in an effective way to gather information about a company and its employees. If this function existed in the most popular search-databases, it would be possible for information to be sold to a third party or to be used in its own organisation. The people that use this service leave information about their home Internet address and what kind of information they are looking for. This information could be used when a company is investigated.

8. Get access to competitors' internal WWW-pages, etc., with a false identity or an identity used by the competitors' customers.

By accessing information in internal mailing lists, WWW-pages or newsgroups, even more information about a company can be gathered. This possibility also gives the opportunity to act in an aggressive way, by, for example, asking questions of a competitor in front of its customers, "when is the function x available in your products? It already exists in the products from y and z". Usually the competitor only listens to the communication. The means to gain access to these internal resources is a false name or identity which is used by the targeted company's customers.

In some cases a company puts up certain access lists so that only certain domains, e.g. schools or only computers in their own country, can access its resources. This kind of restrictions can typically be related to information regarding co-operation between the school system and companies, or in more specific legal areas such as cryptography. In these cases a public proxy-server belonging to the domain granted by the access list can be used to by-pass these restrictions.

9. Map a competitor's internal network in connection with projects or consultancy.

Mapping of computer networks in connection with joint-ventures or in connection with consulting services will help a competitor to make an inventory of the company's IT-infrastructure, learn external connections to customers, and to enable it to investigate and access available information. Normally this is no problem, as the consultant asks what services he can use (product information, workflow, administration) and within that framework he can move freely without any risk of getting caught.

Among the most important information within a company is market analysis and strategies, both short term and long term. This information is normally available in databases, file servers and workflow systems. The information often exists in many different places.

10. Intrusion

The aim in secret, is to get strategic information, orders, tenders and technical know-how. It is important to know that intrusion in the internal systems of a company is not the only way to get access to the systems. It is possible to manipulate the traffic in DNS-servers and routers beyond that company's control. It is also possible to eavesdrop traffic between the competitor and its customers and partners on the Internet.

Information Warfare

Information Warfare has earlier been implemented in politically related issues and has only occasionally been observed on the commercial side. With Internet the use of Information Warfare is applied more directly towards competitors, and is becoming common practice when it comes to gaining market share. These methods have also been used by organisations. There also exist "military definitions" of IW, mainly beginning at the very end of this list. These definitions will not be related to in this article. Another important aspect of IW is to be able to detect and analyse campaigns against your organisation at an early stage. The following table describes the methods being used on the Internet, and is graduated according to the same principle as previous graduations.

1. Use the Internet to publish information and services.
2. Strategy over keywords in search-engines, with relevance to number of hits and excluding competitors.
3. Use the Internet to spread objective and "scientific" information
4. Put restrictions on own employees' abilities to communicate on the Internet
5. Put up and maintain FAQs
6. Use the Internet to spread subjective and "unscientific" information
7. Reservation of domain names
8. Intrusion in WWW-servers with intent to change/sabotage the presentation
9. Denial of Service attacks
10. Steal information from the competitor with the intention of publishing the information on the Internet.

Points 1-3 can be regarded as normal IW-activities. Points 4-5 is a more aggressive stance, which in certain conditions can be questioned from a moral and ethical point of view. Points 6-7 are directly questionable and points 8-10 include only illegal activities.

A deeper analysis of the IW points

1. Use the Internet to publish information and services.

The Internet could be used very effectively for publishing information. The cost compared with sending information through postal services or presenting it by means of seminars is very low. These benefits are, however, also available to all companies. In the IW perspective the Internet is a new battlefield for established companies as well as an opportunity for new companies. Companies with publishing experience find it easier to understand the need for a professional attitude and consistent presentations. Information is most often stored on Web pages in HTML format. These are connected with other web pages via links. It is thus possible to set up links to both customers and competitors. In normal cases a company wants to publish its own information and present its services. In order to help customers to find this information, index servers and the home page (often

given by the easy to remember construction www.foo.com) are used. The web page could also be used to provide addresses, current prices, offers, seminars and presentations.

2. Strategy for keywords in search-engines, with regard to the number of hits and excluding competitors

Information on the Internet is often found with the help of search tools, such as web crawlers. In order to find a product it is necessary to provide a "key-word", for example the name of a product or a company. Most web crawlers present the search results with respect to the number of occurrences of the key-word in the text, how early it appears in the text, if it is part of the page title or other titles within the text.[8] In addition, some web crawlers present meta-information in the form of a list of keywords together with a short description of the content.

In order to create a strategy for search tools a company must understand the market, their customers and their competitors. It must be easy to find the required information in the web presentation as well as with different public search tools. Keywords could be selected from common branch vocabulary, product names, words often used in index servers and finally competitors' choices of keywords as indicated by their meta tags keywords. For each keyword comparisons should be made with a different number of search engines in order to evaluate the ease of finding the web pages compared with the competitors. It is important to realise that the selection of keywords is not static, all companies and organisations are interested in a good position in searches and adapt their presentations accordingly. It is also good practice not to give a high search score to web pages of minor importance, since the company may be manually excluded in the next search.

Another possibility is "flooding" with a larger number of web pages and well organised keywords in order to come before competitors or organisations opposing a specific project or product. This can also be regarded as one kind of Denial of Service attack against the search database regarding one kind of subject, because it is in a way possible to destroy every single person's searches in a specific area by flooding a subject.

3. Use the Internet to spread objective and "scientific" information

Some of the first information a company puts on the Internet is objective information regarding their own products in the form of technical descriptions, specifications, white-papers and descriptions of typical usage of their products. In this process research papers and engineering information could also be distributed together with links to similar information sources.

Objective and scientific information can be used to build credibility, not only in connection with their own products, but in the entire field in which the products exist. For example, a manufacturer of a certain product can manage an information database on the scientific improvements in a certain field closely related to the product the company manufactures. The information can be objective, since it does not have any direct connection to the product itself and cannot be in conflict with the company's strategy. If the company maintains this database, it will soon be an authority in that field, and the product becomes synonymous with the credibility of the database.

4. Put restrictions on employees' abilities to communicate on the Internet

The presentation of a company on the Internet could be negatively affected by a large number of employees presenting their views of the company, its products and its relations to competitors, customers and the market. It is important from an IW point of view to let the information department handle these types of questions.

In most cases young employees have been the first to use the Internet. The new opportunities for a larger number of people to represent the company, and changing social values have increased the threat of uncontrolled IW. Information written hastily and informally could cause a company great problems before they are identified by senior management. When competitors and customers reply to news postings or e-mail, conflicts could easily arise and develop. How information is treated differs between different companies and countries. Companies that have a more mature view towards Internet usually put one or more of the following restrictions on its employees:

- All public services and information destined for the Internet must be approved at corporate level, e.g. the Information Department. (Information classification)
- Ordinary users cannot mail on use-net news. All communications to newsgroups are managed by the information department.
- Restrictions on communicating with e-mail. Only sales and managers are issued an e-mail account, accompanied by certain restrictions on usage.
- Restrictions on employees' using the Internet, getting and obtaining information. Access goes via proxy-servers and access-restrictions are often applied.

These rules are implemented and enforced to different degrees dependent on country and corporate culture. It is important to notice that these measures do not only have positive effects, and might backlash to become the opposite, including bad will and exodus of creative staff. These measures are dangerous, because if implemented wrongly, the company/organisation becomes vulnerable.

5. Put up and maintain FAQs

In the beginning of USENET it was observed that certain questions were asked very frequently. In order to decrease the traffic in the newsgroups (each question generated a number of answers) it was soon general practice that each newsgroups should a have a FAQ (Frequently Asked Questions) document. This document begins with a section of all questions in a number sequence followed by one or more sections with answers to the questions. The FAQ is handled by a FAQ maintainer who on a regular basis gathers new questions and replies from the newsgroup and incorporates them in the FAQ document. This document is normally posted at regular intervals to the newsgroup. All FAQ documents are also mirrored at a large number of sites, this being an important and valuable document for solving problems or searching for further information.

As commercial interests have increased on the Internet, there are FAQs handling questions related to commercial products and services and the usage and advantages of different solutions. A company that maintains a FAQ could make comments or present the problems and solutions in a manner that follows and supports their own product arguments and marketing.

By creating a newsgroup or mailing list it becomes possible for a company to maintain a FAQ document at the same time. Ordinary newsgroups on USENET are supposed to be objective and non-commercial, but this is difficult to maintain. As companies restrict their users' abilities to post information to the newsgroups, the company could have a great influence on FAQ documents and seminars regularly presented to the newsgroup.

6. Use the Internet to spread subjective and "unscientific" information

In most cases companies provide links to web pages in favour of their products together with links to retailers, business partners and large customers. Subjective information could be presented as customer interviews in web pages, complaints against the competitors' products in newsgroups and

mailing lists, or recommendations for the company's own products. In these later cases anonymous mailers, forged mail traffic or mail accounts not related to the company are used.

A method that is more subtle, is to use science as a means of marketing. Before Internet became commercial, it was used as an information exchange network between universities. This led to standards on the writing of scientific reports, i.e. fonts, layouts, margins etc. The format has led many people to believe that a report on the Internet, following the standards, has scientific integrity. Those reports are written in an objective way but distort facts or use facts in wrong contexts. The reports are written by people who have a deep knowledge of the subject in question. Only people with similar knowledge can verify the quality of the reports. The reports are often released in newsgroups, with high attributes, which leads to wide distribution on the Internet and become publicly available on FTP sites and ordinary users' home pages. In most cases the reports originate from the company itself, but in some cases scientists at universities are used as 'fronts' to give the report additional integrity. This has led to real scientific reports and "unscientific" reports being mixed together, even on very selective archives.

Using the techniques in point 4 of the BI-explanations, a company can detect which customers, vendors or organisations have links to its web pages. By first presenting good objective pages and scientific information, the results will be that many educational sites and independent organisations put up links to companies' web pages. The company can now change this information, so it becomes more subjective. The links from independent sites still remain, and the company can market its own products via independent resources.

7. Reservation of domain-names.

The Internet has been growing chaotically, and it has been relatively easy to register domain names. It has specially been related to so called .com addresses. The normal competition has been among names relating to products or brand names, i.e. www.sportcars.com which could be a good name for a manufacturer of exclusive sports cars. The name has the attributes of being easy to remember and at the same time partly excluding its competitors.

A company with a big or dominant share of the market might be tempted to register the common name of that particular product as an own domain. It is also common that these names are registered as a pre-emptive action. It is maybe not correct to use the name, but the company will not risk a competitor or an organisation doing so.

A more aggressive way is the fight of domain names or registering domain names that can be sold in the future, or domain names that can cause damage, i.e. names that are connected to deregistered companies or brand names that are still widely known.

A domain name can also be used to track users trying to get information from this domain. This can be used in connection with BI finding new customers.

8. Intrusion in WWW-servers with intent to change/sabotage the presentation.

The web server must be available to Internet users. It is therefore possible for an outsider to investigate the server from a number of aspects. The pages in the server must also be easy to update. It could be possible to listen to the networks with sniffing techniques for passwords and user-ids. The web server is often placed outside the corporate firewall. One of the larger vulnerabilities is its links to interactive scripts.

Modifying web pages on the Internet is in most cases regarded as graffiti. It often results in bad will, i.e., the intruder has shown that the company or organisation has poor security on its servers.

A more subtle attack is when the server is attacked and only minor changes are made to the information, i.e., changing important key factors in the information. The changes may be a "misprint" in a report, such as key values that show a fiscal situation or the performance of a product. This "misprint" may exist a long time before anyone recognises the problem. The person who is relying on this information can make wrong decisions, which in the long term can lead to catastrophic consequences. For example, the company presenting the information will then always have worse figures than its competitors and will in this way lose customers. The problem is that more and more people rely on and believe the information presented on the Internet.

9. Denial of Service attacks

Denial of Service was earlier regarded as an internal and unintentional threat to mainframe computers. As companies are becoming more and more dependent on external communication Denial of Service has become a distributed problem. Denial of Service is a term that describes when a failure in a system results in the system's ability to deliver a service decreasing significantly or ceasing to exist.

In an IW-perspective an organisation's connection to the Internet or any other global network is highly important in a critical situation. A critical situation can be when the company announces or releases a new product or when failures are found in a specific product, and the company is dependent on delivering fixes and information about the failure. At the same time competitors are using the failure in their own market strategy. As companies and financial corporations uses the Internet for electronic money transfers, the aspect of availability is even more important.

To protect the internal networks against the Internet many corporations/organisations use a Firewall of some sort. The Firewall's purpose is to protect, in many cases, the entrance/exit to Internet. All communication is passed through the Firewall, and it is often configured in such a way, that if the Firewall fails, all communication with Internet fails.

Denial of Service attacks can be launched in many ways and it is not necessary to crash a server to reach the goal of an attack. The ability to cancel newsgroups and other people's messages in the newsgroups is one example. Some FTP-servers only allow a certain number of anonymous users. This service can easily be blocked or decreased by keeping as many as possible active anonymous sessions active against that server.

When the objective is to actively crash servers and services, simple and effective methods can be used. Such attacks are usually used successfully against firewalls, and the attack results in total failure of the connection to the network. The attacks mentioned are related to failures in the implementation of the IP-suite.

- SMTP and NNTP flooding - is used against mail, news or combined firewall servers. The purpose is to overload the server with more mail and news than it can handle.
- TCP and UDP packet storms - more packets than the server can handle are sent under a short period of time.
- SYN-flooding - Blocking the server with TCP-SYN packets.
- Ping of Death - a common failure in most systems, sinks the server when long ping requests are used.
- ARP-flooding.

The attacks often result in that the service stops, and the only action needed is a restart of the server or service. In some cases it is possible to crash the machine completely.

10. Steal information from the competitor, modify and then publish the information on the Internet through anonymous channels.

To steal information from a competitor as a step in a company's IW-strategy is more often observed on the Internet. The cases observed have often been used by terrorist groups or by non-governmental organisations. The stolen information has in most of the observed cases been regarded as unmodified. The publications stolen in the observed cases have led to great costs, endangered human lives or led to bad will [9]. The information may also be modified before it is published. Often small changes in the information are more effective when conducting IW. The small changes mean that the focus of the document is changed in favour of the attacker, but still keeps its reputation for integrity and reliability of information.

Discussion

The first important factor is to understand the new methods for conducting BI on the Internet, and reduce the consequences if such methods are used against your own organisation. In the past the most common classification of information was confidential, internal and public. But a new classification scheme may be necessary, since new search tools and web crawlers have made the Internet work like a large database. In this scheme public documents should be divided into documents that could be provided through the Internet and public documents that should not be provided through Internet, or otherwise restricted.

The next important factor is to detect at an early stage negative information that could be the start of an IW type of campaign against your own organisation. The reasons for a competitor to support a campaign could be a struggle for a new industrial standard, breaking a monopoly situation or gaining a new market share. Reasons for an organisation to build up a campaign could be based on political, social or environmental reasons. Information supporting campaigns could include discussions with involved parties, general understandings, economic facts or reports describing consequences. Campaigns are often born in newsgroups and mailing lists. It is sometimes possible to foresee a campaign and the arguments that will be used some time before it starts. When the campaign has started it is easier to detect, due to a large number of replications of texts to a large number of sites. If the campaign is directed against a competitor it is still of importance to understand the reasons and see if it may affect your own company.

The stated BI and IW points show that the Internet has different rules concerning BI and IW, from traditional means of gaining and spreading information.

- The information presented is never fixed. A document, report or presentation can be changed without notice.
- Information once given to the Internet is difficult to extinguish, as it may be stored, replicated or indexed on other servers for a very long time.
- There are no global ethics, rules or laws regarding the spreading of information.
- Everyone has the right to publish and collect information.

The simplicity of conducting intelligence activities and information warfare on the Internet, as described in the BI and IW points, gives a single person or small organisation the means to achieve the same credibility and power as a major company or organisation.

Conclusion

The Internet is still a relatively new phenomenon and it will take some time before all possibilities and consequences are realised. Business Intelligence and Information Warfare is a field which is increasingly used by companies. The terms "computer security" and "data security" are modified to mean more or less information security. Security is no longer a problem that can be solved with technical means, but demands a greater responsibility and surveillance of the information on the Internet. The Internet has given new opportunities to get information, but it has also given an unlimited number of ways to manipulate, market and gain information without breaking into or damaging systems.

References

[1] *"Security Forms for Protection against Vulnerabilities in Computer Systems", E. Johnsson, Tomas Olovsson, Department of Computer Engineering, Chalmers University of Technology, Gothenburg, Sweden, 1992.*

[2] *"INFORMATION SECURITY Computer Attacks at Department of Defence Pose Increasing Risks", United States General Accounting Office, May 1996.*

[3] *"The Business Intelligence System: A New Tool for Competitive Advantage", Benjamin Gilad, Tamar Gilad, AMACOM, American Management Association, 1988.*

[4] *Lecture Notes in "Business Intelligence and Security", Stevan Dedijer, Department of Business Administration, School of Economics and Management Lund University.*

[5] *"Propriety Information: How It Leaks Out, and What Can be Done to Protect It", Chemical Engineering, 23rd May 1966, pp 160-161.*

[6] *"Hypertext Transfer Protocol -- HTTP/1.1", http://www.w3.org/pub/WWW/Protocols /rfc2068/rfc2068.txt*

[7] *"TCP/IP Illustrated Volume 1, The Protocols", Richard Stevens W, Addison-Wesley Publishing Company, 1994.*

[8] *"Advanced Searching: Tricks of the Trade", May 1996, http://www.online.com/online /onlinemag/MayOL/zorn5.html*

[9] *"alt.scientology.war", Wendy M Grossman, Wired Magazine 3.12, December 1995*

Mikael SIMOVITS

Works as a Management Consultant for ICL, building consulting services around computer and information security. He begun his career as cryptoanalyst, and then worked toward the field of network and information security. He has published the following material.

"The DES, An exhaustive Analysis and Evaluation of the Data Encryption Standard", Ageean Park Press, 1994
"Secure Remote Access", *SIG-Security 1996. (Swedish) Together with other authors.*
"Business Intelligence and Internet", *Nordsec96, 1996. (Swedish) Together with Tomas Forsberg, ABB Infosystems AB.*

Tomas FORSBERG

Works as a Management Consultant within ABB Group, working with IT-security related problems. His experience around the field of IT-security is vast and ranges from Mainframe security to Network and Information security. He has published the following material.

"Business Intelligence and Internet", *Nordsec96, 1996. (Swedish) Together with Mikael Simovits ICL Svenska AB.*