

## Dealing with Internet risks

Vasilios Katos\*

Cambridge Technology Partners, The Global services Company of Novell Inc.

### Abstract

*This paper discusses the attitude of both e-businesses and e-customers or perspective e-partners towards the risks which are born by using the Internet as the communication channel. The risks are highly correlated and shape the trust of an e-customer towards an e-business. Starting from the organization's attitude towards risks, a number of criteria that influence the customer's trust are presented.*

### Introduction

On the November the 2nd, 1988, the Internet suffered from a systematic attack from the "Internet worm" [1]. The day after was named as "Black Thursday" because approximately 70% of the interconnected systems were out of order. This event triggered the systematic attempts to add security operations to the Internet, which was regarded as the most successful medium of information offer and retrieval. In fact, security issues had never been mentioned before the attack of the worm.

Twelve years later, at the dawn of the twenty first century, history repeats itself on a different scale. The popular site yahoo.com experiences a denial of service (DoS) attack and thousands of users did not have access to their electronic postboxes. Some days later, a known financial institution that provides web banking to its customers, allowed users to access all customer records due to a programming error. Such an event was a clear breach of confidentiality and it appeared after an upgrade of the web banking software.

Several months ago the NIMDA worm toured around the Internet, with the ability to affect systems that used Microsoft's email products and the Microsoft web server, IIS.

### Analysis

There is a fundamental difference between the operation mechanisms for the 1988 worm and the attack at yahoo.com. The worm leveraged the internet protocols in

combination with the discovered vulnerabilities of the operating systems; the majority of hosts were running under Unix. In the case of yahoo.com, the attack was based solely on the vulnerabilities of the internet protocols and more specifically on the TCP handshake stage.

The DoS mentioned above could have been executed with success at most Internet sites, since confronting such an attack is difficult and requires a coordinated effort of a number of components, including an intrusion detection system, cooperation and timely response of the Internet Service Provider, as well as availability and instant response of the site administrator. Yahoo.com was probably selected for the attack because it is one of the most popular and commercially successful sites, with the potential to affect thousands of users. Therefore a successful attack would give a greater satisfaction to the attacker than a less popular site. Of course the attack could have been mounted from - or behalf of - competitors or from parties who could have financial gain, but this has not been established.

It can be argued with a considerable degree of confidence that the security of the interconnected systems is much higher than the security of the systems that operated twelve years ago. Today a firewall is a typical network component which is exposed to the public network. Furthermore, many organizations have approved the Internet to be used as the channel to reach their customers, partners, or employees. So why do large scale security related problems are still in the picture? Why do these security breaches make us realize that the perceived security level of our system is much higher than the actual security?

The answers can be found in the common characteristics of the two epochs we are comparing. The main characteristic is the very existence of the Internet: the need for interconnection. No matter how many security measures are placed, there must always be a port open, our electronic reception to serve our customers. The Internet has become an entity which has developed immunity to various assaults, but remains vulnerable to new ones. As in pharmaceuticals research and development is needed for the creation of new antibiotics to treat the new diseases, similar activities are required to deal with the new threats in Cyberspace, i.e. the creation of new defense mechanisms.

One other common characteristic of the two epochs is the perception of the security issues and the "it cannot happen to me" syndrome. This characteristic is also apparent in the health sector with the numerous education and awareness campaigns, which aim to change the culture of the public towards some diseases. There is an analogy between a company dealing with IT security issues and a human dealing with health issues. There exist companies which do not consider security to be an important matter and react only when they are affected. There are companies which have a knee-jerk reaction and pay high prices in order to

cure their system. However, there are also "hypochondriac" companies who believe that are constantly under attack and consume their resources in order to apply every possible solution which is available on the market, without considering its applicability and usability. Finally there are companies who have taken the appropriate prevention measures and also react with prudence in the case of a security breach.

An important conclusion is derived from the above, with respect to dealing with Internet risks and consequently with trusting the Internet, since trust and risk are terms which are highly correlated and can be interchanged. The conclusion is that a statement like "I do (not) trust the Internet" is not applicable. The Internet is an information propagation medium and therefore it would be unfair to tax with its operation means. Besides the Internet was not designed with security in mind. On the contrary, trust must be referred to the companies and more generally to the end systems with which we perform transactions. When we feed our credit card number in an electronic form and send it to buythebook.com, the SSL security protocol which is supported today by all browsers, is adequate to preserve the confidentiality of the credit card number during its transfer over the Internet. The real security problems arise by the time the number arrives at the systems of buythebook.com, where we do not know the number of locations our credit card number is stored, the location of the database(s), as well as who has access to the database(s), whether she is a company's employee or an external party and in general how the company is dealing with this sensitive information.

Consequently, in order to have cooperation and eventually a sustained relationship between an e-business and a customer, the former must meet the trust expectations of the latter. In the world of e-business the characteristics which influence and shape the trust of an organization include:

- The presence history of the site. As a rule of thumb, the older the site the higher the trust. This can be combined with the fact that if the site belongs to a successful and known company, then the presence history is expanded.
- The site's attack history and the company's reaction towards the attacks. More specifically, the company's response time following a security related event is an indication of the organizational readiness towards external threats. Furthermore, when multiple sites suffer synchronously from advanced attacks, the response and recover time is a very important differentiator.
- The existence of a privacy statement, as well as the existence of the security policy statement. These statements must be placed in easy-to-reach locations, without requiring the user to consume considerable time to track down the links to these statements.

- The application of the security policy. Although the procedures and security mechanisms of the systems must be transparent in order not to discomfort the legitimate user, from a trust perspective the presence of the security mechanisms is essential. For example, the existence of a password policy could be succeeded with a respective web page educating the user about the password rules (e.g. minimum number of characters, denial of use of names, etc.)
- The financial and accounting information of the company.

## Conclusions

Although there are risks associated with the use of the Internet as the enabling technology for doing business, most of them can be mitigated with an organised and systematic security investment, including both technology and organisation. Since these risks depend on the security awareness and responsibility of the underlying e-business organisation, it follows that trust should refer to the organisation rather the internet itself. A number of characteristics which indicate the security behaviour of a company were listed. However, this list cannot be complete since it is generic and not industry specific, and also the e-business environment is dynamic.

## References

- [1] Don Seeley, *A Tour of the Worm*, <http://packetstormsecurity.nl/papers/virus/tour.ps>

---

\* Dr. Vasilios Katos recieved the MEng degree in Electrical and Electronic Engineering from the Democritus University of Thrace in Greece in 1994, the MBA degree from Keele University, UK in 1995 and also received the PhD degree in Computer Science from Aston University, UK in 2000. Since 1999, he has been working as a Security Architect for Cambridge Technology Partners, the Global eServices Company of Novell Inc. His research interests are cryptography, e-commerce security and risk management.