Researching and Structuring e-mail Security Criteria

Mario Sajko, Miroslav Bača
Faculty of Organization and Informatics,
Pavlinska 2, 42000 Varaždin, Croatia
Phone: (385) 042-390-800 Fax: (385) 042-213-413 Mail: {mario.sajko; miroslav.baca}@foi.hr

Tedo Vrbanec
Faculty of Teacher Education – Centre Čakovec
Dr. Ante Starčevića 55, 40000 Čakovec, Croatia
Mail: tedo.vrbanec@gmail.com

Abstract – Validity and efficiency of e-mail use in business communication have not been disputable for a long time. But what is disputable is security and risks of e -mail use. It is in danger because of threats coming from different sources and forms of work. E-mail content, computer data, corporative networks as well as business processes and image and partner's trust can also be in danger. This paper highlights proportions of e-mail (in)security in business environment. E-mail security strategies and technologies, as well as their limitations are being discussed. As a recommendation for e- mail security managing, the role of security policies is being explained as well as the need for defining criteria that are missing in practice. After researching the best experience, security standards directions, and business process features, e-mail security criteria are structured and the ways of their implementation in business environment are shown in this paper.

I. INTRODUCTION

We can't imagine the world today without e-mail use. By e-mail we do our private and business correspondence, use it to coordinate work/tasks/assignments among the employees and work groups as well as to transfer files. E-mail is an important part of *e-business* [12], [16] in which it is used for communications among companies. In business organisations daily operative businesses, meetings, qualitative decision making and critical business processes depend on it. That is the reason why e- mail is particularly the most important internet service.

While every day we exchange textual and pictorial recordings, sound and animations by e-mail, at the same time we open the door to many dangers for our business. Namely an e-mail is the easiest way to distribute dangerous contents on personal computers and corporative computer networks. While using e-mail there are some security threats that can come out from the computer network and there are some specific qualities coming out of the way e-mail is used. Potentially the biggest e-mail dangers come out of the fact that e-mail is the content carrier, especially when talking about the files of different types.

In the last few years the danger of malicious programs (viruses, *Trojan horse, spam, adware, spyware, worms* etc.) has widely spread in the internet. Such unwanted programs can be infiltrated on computer using e-mail as a carrier. The most common aims of the malicious programs are deceit, leading to reveal personal data, infecting computer, taking the control over computer or just disturbing of normal work. The authors of these programs are inventive hackers who are trying to get their personal benefit or spite the computer users. The sources of the malicious programs are mostly unknown and can come from the Internet pages that we have just visited or from already known but infected source.

This is the reason why the messages received by e-mail can potentially be a dangerous source of incident (corruption or data loss, systemic software, unauthorised access to data, data thefts). Beside this, the incident can result with the other damages as passing e-mail to wrong addresses or passing the wrong content to the right addresses. Such situations can lead to a loss of personal or business respect.

9 of 10 received e-mails in the world of the estimated 15 billion [11] daily e-mails [14] are spam. Spam is a form of threat for e-mail service although they are not malicious in their character. Their harmfulness lies in the fact that they unnecessarily burden the Internet business, burden the user and his system, time spent working with e- mail and finally lead to unnecessary costs. The costs of spam messages cause an additional unnecessary cost ($1,000 a year per employee) and they also decrease productivity and computer costs [14].

Legal regulation dealing with malicious programs and with spam messages doesn't have the expected success. It seems that neither laws nor security program solutions solve the problem of safe e-communication. This paper is based on this idea and view. It seems that one of the e-mail security problem components is man, his way of approaching and using of e-mail. So the problem should be solved if we start with human side, their way of behaving and security practice [20], [22]. This paper explains the way how to control and promote e-mail security. The basic starts in problem solution are universal security criteria that can be found in internationally recognized standards and e-mail security policy coming from different sources. The idea and hypothesis of this paper is that by upgrading security criteria recommendations and e-policy and their combining with already determined features of a business process we can create the basis for acceptably safe use and e-mail security managing.

A. Experience with e-mail security and threats

Nowadays the threat with computer viruses is not so noticeable because of the high efficiency of antivirus programs as well as their ordinary use [9]. Although they can disturb in working, spam messages also do not make direct damage to business. Today the biggest danger through e-mail use, is the possibility of deceiving a receiver (in the sense of making profit) or to reveal confidential information (e.g. through sending to the wrong addresses) and also inappropriate protection of sensitive information. In numerous conversations with e-mail users and systems engineers it has been shown that the users are very often neither familiar with, nor are they aware of these threats. Even if they are familiar with the above mentioned threats, they do not have enough competence, authority and/or desire to start action to decrease security risks.

TABLE I
OBSERVING RESULTS OF E-MAIL SECURITY THREATS [9]

Type	Percentage	monthly increase	Annual Average
Spam	In 64.4% emails	0.1%	58,13%
Viruses	One in 89.6 emails	0.1%	-
Phishing	One in 170 emails	0.27%	-

According to the research [7], 11% of users use e- mail in a wrong way, and in some bigger companies this percentage is even higher. They believe in the efficiency of their programe protection and the defence strategies from unwanted contents. But the fact is that these threats are often bigger than they are supposed to be.

It should be known that by e-mail messages the weaknesses of pop, imap and mail protocols that operators use for exchanging e-mail can be rather easily used. Beside this, newly appeared threats are avoiding the existing security implemented by the operators. E.g. a typical firewall can not protect from the e-mail message attack as it does not analyse its content. Furthermore e-mail filters are not efficient enough as new threats are appearing daily. In addition to this, technological and program solutions that are appearing every day are not suitable to an average user.

The most common sources of risk that are usually listed as security incidents caused by e-mail, are the following [18,19]:

- Eavesdropping
- Spam or Unwanted Email
- Viruses and Worms
- Email Logical Bombs and Other Attacks
- DDoS Zombies
- Pranks
- Trojans
- Social Engineering
- Hoaxes.

The most common causes of dangers the source of which is a user and which generally appear because of irresponsible or irregular e-mail use are:

- e-mails are not coded in general, so on their way from the sender to the receiver they are passing through other computers and it is easy and simple to intercept and read the messages
- on one hand, the header of the message has data which make it impossible for an average user to have anonymous communication, and on the other hand it is easy for the malevolent user to falsify the header and to make a false presentation
- through the infected computers that are controlled through the Internet with the help of unwanted program additions, Trojans or software for momentarily messages, the operation is malevolently blocked by unwanted or infected e-mails
- security propositions of software that is used are not adequately set
- users incautiously and without checking open e-mail as well as the dangerous Internet pages
- an average user is not educated and conscious of the need for regular updating of system and user software, so he is not implementing it: the other aggravating circumstance is big ”intensity” of program packages that have to be downloaded from the Internet, which for the majority of users presents an unreasonable and incomprehensible cost

Threats action is a cause of about ten forms of risk that appear for user and /or his data [8]. Among the most important negative influences that appeared by e-mail are [1]:

- vulnerability of messages to unauthorized access or modification or denial of service;
- vulnerability to error, e.g. incorrect addressing or misdirection, and the general reliability and availability of the service;
- impact of a change of communication media on business processes, e.g. the effect of increased speed of despatch or the effect of sending formal messages from person to person rather than from company to company;
- legal considerations, such as the potential need for proof of origin, despatch, delivery and acceptance;
- implications of publishing externally accessible staff lists;
- controlling remote user access to electronic mail accounts.

B. Current state in e-mail security concepts

There are many works dealing with e-mails security from the technology context [18], [23] or general security improvement context [3], or with solutions about avoiding junk mail and spam [4] but also there are numerous strategies and specific program solutions [6], [23].

Nowadays a very common example of struggling with e-mail threats is the use of e-mail filtering software. They supervise e-mail messages and when examining their content they keep or filter unwanted contents and messages. There are also unavoidable firewall and antivirus programs. As solutions for removing threats we can mention [18]:

- Encrypted communications
- Privacy policies
- Anonymization
- Spam firewalls

There are not many data about experience with e-mail security coming from business environment. Security practice research on the developed market of Great Britain shows that incoming e-mail security is rather common while outgoing e-mail security is not so common [7].

The encryption of the outgoing mail is practiced only by a quarter of the employees in British companies, only a sixth of UK companies scan outgoing mail looking for inappropriate content. The research shows that some mistakes also happen by accident e.g. sending confidential information to the wrong addresses. It can be seen that in spite of awareness about the dangers that are brought by e-mail use, many companies do not protect e-mail enough (or not at all) from the security threats. In good practice the big corporations that have security practice better and more rigorous set an example.

TABLE II
PERCENTAGE OF COMPANIES THAT ARE UNDERTAKING SECURITY MEASURES FOR E-MAIL PROTECTION [7]

Type of risks	Incoming emails	Outgoing emails
viruses	94%	70%
spam	86%	-
inappropriate content	-	10%
block or quarantine suspicious e-mail attachments	96%	-
confidential information	-	13%
unencrypted information that should be encrypted	-	8%
no scans	-	28%

What is missing in similar research are more precise data about (financial) losses and costs that arise from e-threats activities. What is also missing are data about the consequences that appear because of insecure e-mail use from the side of user.

C. Outline

The further part of the paper relates to establishing the criteria that will serve for integration of the Internet security policy and testing methods of implemented security controls (Section II.). What is still unknown is the structure and content of such criteria, testing methods of their implementation as well as distribution and responsibilities areas for security in business environment. Section III shows strategy example for e-mail criteria implementation. Finally, section IV gives a conclusion.

II. E-mail security Recommendation

In spite of technical and program solutions, the risks in e-mail use still exist, and the threats all the time find new ways to use the weaknesses of defence. The problem is that in spite of the achievements of security solutions and measures their successfulness still depends on the attention of users that they give to security. The idea presented in this paper is the necessity to adopt the security concept where users present one of the lines of defence and business information protection measures.

In practice e-mail users behave in accordance with their knowledge of security problem area and the use of program solutions for security. Nowadays the solution for the advancement of security practice is often sought in the norms and security standards (ISO, BSI, NIST, GAO, FIPS, DoD, etc.). Although they only touch the e-mail security question (e.g. ISO mentions e-mail security in paragraph 8.4.1.) such security criteria model is applicable in developing e-mail security. What should be defined in security criteria is:

– proceeding of business processes under e-mail
– influence or that are proceeded by using e-mail
– introducing the staff to the potential consequences of inappropriate, risky or damaging e-mail use
– preventing the staff to use e-mail in inappropriate, risky and damaging way
– provide e-mail use with reasonable burdening of information system resource.

A. E-mail security criteria

Security policy is an instrument by which the management usually provides the implementation of security measures and support to users and provides directions for managing security. It is a common practice that big corporations have an elaborated e-policy (internet service use policy) and even an e-mail policy (e-mail use in business). But, determining the obligation to apply the security policy directions does not mean that the defined policy would be used. In reality the care of e-mail security is ceded to final users or administrator.

If we analyse the examples of different e-policies and less frequent ones, it is obvious that they are not enough oriented towards business processes but too much to general recommendations. With this they do not give a precise answer to what is expected from the user in the sense of responsibility. Because of that they can cause neglect and indifference. There is also a need for explicit recommendations that do not leave space to dilemmas. Such directions should be formed as a group of rules or criteria that should be considered (implemented) or they have to define clearly what users are and are not allowed to do [21]. The example of some of the “good practice” rules or areas that have to be covered with e-mail criteria are [3], [13], [21]:

- Scan incoming and outgoing e-mail messages
- Implement software to monitor Internet usage and block inappropriate sites
- Protection of electronic mail attachments
- Guidelines on when not to use electronic mail
- Use of cryptographic techniques to protect the confidentiality and integrity of electronic messages
- Retention of messages which, if stored, could be discovered in case of litigation
- Create rules for permitted use
- Virus and content filtering
- Implement system monitoring and privacy
- Employee responsibility not to compromise the company
- Prohibited, illegal, licensed and copyright material
- Sexual harassment, discrimination and defamation
- Reporting of incidents and vulnerabilities
- Etc.

Such and other-mail security use recommendations can be further developed in more detailed rules. Such example is shown in Table III where 6 security rules are defined for two typical e-mail uses.

TABLE III
EXAMPLE OF CREATING E-MAIL SECURITY RULES

1. E-mail should be used only for business purposes, with using expressions that are in accordance with other forms of business communication
1.1. Business e- mail correspondence is done in accordance with declared sensitivity of business information 1.2. Information about users or employees as well as the other sensitive data are not sent by e-mail 1.3. In advance planned and standardised models are used in business communication
2.Input e-mail should be treated very carefully, considering the present security risks
2.1. In opening suspicious files what is considered is the sender's address, message title and type of the enclosed 2.2. E-mail with suspicious content or title (sender, enclosed material, message headline) or text are momentarily deleted from the computer and the threat is reported to administrator 2.3. Opening the files that are added to e-mail is allowed only in case that the message with belonging files is checked and verified from the side of antivirus programe

B. Basic structure of e-mail security criteria

Next thing that should be explained is the way e-mail security criteria structure should look like. Organization of criteria can be started from different points of view. The example of e-mail security criteria structure is shown in Table IV. If e.g. the criteria are structured according to business hierarchy then we can differ the criteria for ordinary users from the criteria that have to be realised from the side of the mail server administrator or IT management.

Which responsibilities can be set in the area of using digital signature? In this case user is obliged to sign all sensitive information. The administrator should provide the infrastructure of public and private key, and a distributor public key filing service, users' support and other propositions on the local Internet access. IT leader should provide education from digital signature use and share obligations concerning its use. His duty is also to define public key use policy. Top management has to introduce and lead a security policy that includes business data protection and also to set obligations of business partners dealing with security communication. Similar examples can be also given for other security areas. One such security criteria division and their decomposition are shown in Table V.

TABLE IV
POSSIBILITIES OF E-MAIL SECURITY CRITERIA STRUCTURING

According to sources of dangers
- Viruses, Trojans and Worms - Instant Messaging - Snooping and Spoofing - Digital Signatures and Encryption - Social Engineering (*phishing*) - Spam - active scripts - network threats (business interception, access to wire and wireless network, DoS)
According to business hierarchy
- ordinary user - administrator - IT leader - senior management
According to types of risks that appear
- Malicious code protection - Unauthorized access protection - Loss of confidentiality - Responsibility and duties - Spam and Phishing

III. IMPLEMENTATION OF E-MAIL SECURITY CRITERIA

The suggested list (Table V) gives the rules that are recommended to be implemented for e-mail security. The job of implementation is realised by administrative staff and final users and/or the one who is involved in the mentioned controls. The job can be divided in two stages:

- (1) monitoring the share of security controls used in practice
- (2) monitoring the efficiency of implemented controls

For monitoring the use of security controls and also for determined self-control and achieving employee's awareness, it is necessary to measure the level of acquired controls. The job can be done by using survey questionnaires. It is suggested to form the so called *check box* (Table VI). The questionnaire is formed on the base of security criteria (and possible sub-criteria) and it gives possible answers: yes, partly yes, no, I don' know as well as a possibility to give the reason for writing nothing. The results obtained by this questionnaire will serve as the instrument for qualitative e-mail risk assessment, as the proportion of necessary and implemented security controls points at the level of (in)security of information property.

For monitoring efficiency and quality of established criteria in increasing e-mail security it is necessary to develop determined quantitative indicators. Their choice is also determined on the base of recommended security criteria. In choosing the right criteria we should above all make performance monitoring possible in the determined period of time.

TABLE V
E-MAIL SECURITY CRITERIA STRUCTURE LIST

IT management	**IT administration**	**User**
– A manual with a glossary for (secure) e-mail use has been made – Public and private e-mail use categories and the way how to use them have been defined – Sensitivity levels of business information and required security level in their e-mail distribution have been defined – Standard e-mail models for business communications have been defined – Signatures containing disclaimer statements about restricted responsibility and obligations have been defined and sent with e-mail – Way of classifying business information for e-mail use is coordinated with general security policy – A responsible person for managing security e-mail work has been appointed – Employees are systematically educated about safe e-mail use – Rights, obligations and limitations about e-mail use as well as consequences for employees in case of exceeding allowed authority have been defined – There is a policy connected with the use of digital signature – There is a policy for distribution and assignment of passwords for e-mail access – There is a list of reliable partners who exchange messages by safe channels with us	– Program and technical possibilities have been undertaken to provide safe communication by e-mail service – Limitation considering the size of files that can be sent by e-mail has been defined – Regular examination of quality of pass-words for accessing e-mail has been carried out – E-mail client use has been unified on the level of organisation – Policy and rules about sending advertising messages in accordance with anti-spam legal laws and rule books have been developed – Obligation to use anti-virus and similar tools for detecting dangerous program codes as well as their updating have been defined – Recommendation for safe use of clients for mail examination and their obligation to update have been defined – Policy dealing with spam-messages and use of spam-filter has been established – Employees' rights and licences for accessing e-mail service have been periodically updated – If corporative web interface is set for web communication – Types of files that can or can’t be received or sent through corporative servers – If alternative mail/pop/imap server is provided because of service criticality	– I regularly practice recommendation of e-mail use policy – I find qualitative support considering safe e-mail use available – I set computer security proposition and e-mail client regularly – Updating software (systemic and applicative) is regularly done from my side – I do my business correspondence by using home computer – I always use anti-virus software – All files received by e-mail I also saved on local servers – To increase e-mail use security I use Firewall, antivirus, antispam and antispyware programs – I am the only one who knows my pass-word for accessing e-mail – With business e-mail service I also use other e-mail services – In business communication I regularly use digital signature and cryptography – In e-mail communication I limit myself only to textual contents (I minimise exchange of audio and pictorial data) – I check the authenticity of received e-mail before using it – I understand the notion and meaning of threats as: Adware, Trojan, Virus, Spyware, Worms, Botnets, Loggers, Dialers – While opening suspicious files I am very careful considering sender’s address, message title and type of the enclosed file – I immediately delete from the computer e-mail with suspicious content (sender, attachment, subject of the message) or text and if is necessary I report it to administrator – When encountering unknown threats I report them immediately to the authorized administrator – Before sending I verify the files that I add to e-mail with antivirus programme – Addresses where I send e- mail always have known destination and person who receives them – I always do business correspondence by e-mail in accordance with declared sensitivity of transferred information – There is no information about the users or employees as well as the business data that I forward to other people during communication – I safely store the messages that belong to the category of sensitive information or delete them from the computer – In e-mail communication I use a secret identity – I do not reply to unwanted e-mail

TABLE VI
FORM OF A QUESTIONNAIRE ABOUT SECURITY RISK IMPLEMENTATION

Criteria	Yes	Partly	No	I donˇt now	Why not
IT Management					
Main criteria Sub-criteria …	□	□	□	□	
IT Administration					
Main criteria Sub-criteria …	□	□	□	□	
User					
Main criteria Sub-criteria …	□	□	□	□	

Table VII shows the example of a few indicators used for monitoring determined performances of (*Measurement targets*) e-mail security. The results obtained in that way are the base for qualitative determining of e-mail risk. It will not always be possible to determine quantitative indicators of security performance (e.g. for security criteria concerning subjective assessment). In that case the base for determining the security level can be qualitative assessments obtained by survey.

TABLE VII
EXAMPLE OF QUANITATIVE MEASURES FOR SECURITY CRITERIA

Measurement targets	**#**
Frequency of pass-word change	< from # times a year > from # times
Total of security incident that can be prescribed to e-mail	< from # a year > from #
Quantity of digital messages without digital signature	< from # a month > from # times
Quantity of received messages the source of which is unknown	< from # a month > from #
Number of unwanted received messages a day	< from # a month > from #
Number of viruses received by e-mail by now	< from # a month > from#
Number of spam messages received a day	< from # a week > from #
Frequency of software updating considering e-mail security	< from # a month > from # times

IV. CONCLUSION

There are more and more threats to information contents that are being infiltrated on computer through e-mail service and through the e-mail message content itself. In spite of a big number of program solutions that limit and/or make impossible their influence on computer, some incidents still happen. The cause for what we can find in the behaviour of users whose lack of knowledge, negligence or intention is used from the side of a malicious software to use the weaknesses of the system in an easier way. It is not possible to completely remove the threat that came out of e-mail. User is one link in the defence chain who should recognize the dangers and whose actions could prevent threats to act and produce the incident. Beside the human factors the other risk factor is inconsistent security policy and unfinished rules. These rules refer to the way e-mail is used, incompetence, commodity or laziness of the system administrator that can improve in great deal the condition of e-mail security service.

It is necessary to acquire security criteria that unambiguously direct to good security practice and demand correct work on the side of a user. The answer to the question about the extent of the use of security criteria and whether they give the results or not is in the research of *check-lists* that has to become a component part of work evidence on the computer of each employee. Beside the *check-list* what else is recommended as a source of information about (in)security state or risk size is carrying out periodical gathering of quantitative indicators.

In this paper it is shown how to deal with e-mail security management. The given criteria and the questionnaires formed on the basis of them are the instrument for achieving this target. The continuation of the research in this area will be directed towards automation of the detection of source threats process, and implementation of security controls considering business process features, area and security targets.

REFERENCES

[1] ***: BS ISO/IEC 17799:2000, ISO, 2004.

[2] ***: "Security First and Foremost", 2006., <http://spam.abuse.net>

[3] ***: Improve the safety of your browsing and e-mail activities, Microsoft, 2005, <http://www. microsoft.com>

[4] ***: How to Manage Junk E-Mail, The associoation of support professionals, <*http://www.asponline.com*>

[5] ***: Protecting your network against email threats: How to block email viruses and attacks, Windows Security, <http://www.WindowsSecurity.com>

[6] ***: Protecting your network against email threats, GFI Security Labs, 2006., <http://www.gfi.com>

[7] ***: Information security breaches survey 2006, PriceWaterhouseCoopers, 2006., <http://www.clearswift.co.uk>

[8] ***: Thirty Eight Email Security Risks, Ecommnet , 2006.,<http://www.ecommnet.co.uk/default.asp>

[9] ***: MessageLabs Intelligence Report, MessageLabs, 2006., <http://messagelabs.com>

[10] ***: Monitoring of spam filter's functionality and efficiency, Kerio Technologies, 2006. <http://www.kerio.com>

[11] ***: The compelling case for total email security, Message labs, <http://messagelabs.com>

[12] ***: Wikipedia, <http://en.wikipedia.org/wiki/E-business>

[13] ***: Information Security: e-mail checklist, <http://www.dti.gov.uk/files/file9963.pdf>

[14] ***: CNN.com article: '9 out of 10 e-mails now spam', <http://www.cnn.com >

[15] Bishop Matt: Computer Security, Pearson Education, New Jersey, 2003,

[16] Braithwaite Timoty: Securing e-Business System, John Wiley and Sons, Inc., New York, 2002.

[17] Deise V. Martin at. All.: E-Business-from Tactic to Strategy, John Wiley and Sons, Inc., New York, 2000.

[18] Kangas Erik: Mitigating Threats To Your Email Security and Privacy by, Lux Scientiae, 2006., <http://luxsci.com/>

[19] Krause Micki, Harold F. Tipton: Handbook of Information security management, Auerbach Publications, 2004., <http://www.auerbach.com>

[20] Leach John: Improving user security behaviour, Computers & Security Vol 22, No 8, <*http://www.sciencedirect.com*>

[21] Staley Natasha: The compelling case for total email security, Messagelabs, 2006., <http://www.nframe.com/PDF/TotalEmailSecurity.pdf>

[22] Stantona M. Jeffrey at All.: Analysis of end user security behaviours, Computers & Security (2005) 24, 124-133, <http://www.sciencedirect.com>

[23] Vrbanec T. at. All: Mechanisms of processing e-mail on Linux mail servers, MIPRO International Convention, Croatian Society for ICT, 2005.