ICT SECURITY MANAGEMENT

Jeanne Schreurs, Rachel Moreau

Abstract: *Security becomes more and more important and companies are aware that it has become a management problem. It's critical to know what are the critical resources and processes of the company and their weaknesses. A security audit can be a handy solution. We have developed BEVA, a method to critically analyse the company and to uncover the weak spots in the security system. BEVA results in security scores for each security factor and also in a general security score. The goal is to increase the security score Ss to a postulated level by focusing on the critical security factors, those with a low security score.*

Keywords: Security, Scan, Audit

ACM Classification Keywords:

Introduction

As a consequence of the fast integration of technologies as Internet, Intranet, Extranet, Voice over IP and e-commerce, a companies ICT-infrastructure will move to more openness to the outside world and as a consequence will become more vulnerable for security threats. This offers lots of new opportunities but also creates new threats. That's why focus and responsibility concerning security become even more and more important. The Computer Crime and Security Survey 2005 shows that these are the 10 most frequent attacks or misuses: Virus, insider abuse of net access, laptop/mobile theft, unauthorized access to information, denial of service, abuse of wireless network, system penetration, theft of proprietary info, telecom fraud and financial fraud. Figures show that attacks come from inside as well as from outside the organisation and bring along large costs. Especially unauthorized access and laptop and mobile theft becomes a enormous expense for the companies during the last years. Because of these large costs, companies became more and more aware that they not only deal with a technical problem but also with a management problem. To tackle this management problem, it is quite important to know the ICT-security state your company is in.

ICT security management

Spending each year a certain amount on security measures is not enough. A company needs a total security approach. It is a must to know what are the critical resources and processes of the company and their weaknesses so the can be protected in the right way.

A solution to this is a security audit. A security audit is ideal to detect the weak spots in the ICT security state of the company. Based on the results of the audit, a security policy can be developed, adjusted to the company situation. A security audit can be used to analyse and describe the security level.

1. Security audit checklist

We have developed a security audit, called BEVA. BEVA is a method to analyse critically the company and to uncover the weak spots of the security system. It positions the company on point of the security aspects in the different areas of business functions. We have developed a standard list that covers all aspects of security, structured in 10 domains being:

- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information secuirity incident management
- Business continuity management

Each of these areas consists of different security factors. The factors are in their turn tested on the basis of several subcriteia. Our list for the security factors is based on the standard ISO 17799. The 36 security factors are spread over the 10 domains ,as set forward in the standard ISO17799 model.

For example you have the domain “access control” and in this domain you have the factors: requirements for access, management of user access, user responsibility, control of network access, control access to OS, control of access to applications and information and use of mobile infrastructure.

For each of the 36 factors, a number of subcriteria are formulated. We developed a list of questions, covering the subcriteria we created. The questions are partly based on the “checklists in information management” SDU publishers. (www.riskworld.net/7799-2.htm).

Security Factor Sfi	Importance	Sub Factor	Relevance/weight 1 to 4	Code question	Question	evaluation 1 to 4
Domain: Access control						
Sf20. Business requirements for access controlPremise	B	access control policymanagement	3	20.1	Is the access control policymanagement based on the business security requirements?	3
				20.2	Are aspects of logical and physical access control included?	3
				20.3	Is it clear for users and service providers which rules are applicable?	2
Sf21. User access management	C	registration of users	2	21.1	Is there any formal user registration and de-registration procedure for granting access to multi-user IS and services?	1
		privilege management	1	21.2	are privileges and allocated on need-to-use basis?	3
				21.3	are privileges only allocated after formal authorisation process?	1
		user password management	4	21.4	should the allocation and the reallocation of passwords be controlled through a formal management process?	3
				21.5	are the users asked to sign a statement to keep the password confidential?	1
		review of user access rights	3	21.6	does there exist a process to review user access rights at regular intervals?	4
					Does there exist a procedure to block the	

Figure 1: Questions audit checklist

2. The audit process and the calculation of security factor scores Sfi's and the security score Ss

To collect the information about the current security situation of the company, we start with the questioning of the key persons in the company using the audit checklist questionnaire.

The company determines which systems or processes are critical for them and connected with it, which security factors are important or relevant. An importance rate is given to the security factors from A (low importance) to E (high importance) (see figure 1).

In BEVA, we express the state of security into scores of the security factor (Sfi's). We do this for all the factors and in the end we give a general security score (Ss) over all security factors. We based our security analysis partly on the Marion-AP method.

To evolve to a security factor score, the key persons is asked to allocate a weight from 0 to 4 to the subcriteria of the security factors to indicate the relevance. Subsequently the evaluation starts and the list of questions is asked. Each question is given a score between 1 and 4. (see figure 2). The management team evaluates the company for all aspects on a one to four scale and at the same time measures the importance or relevance of all subfactors.

Security factor Sfi	Security Subfactor Ssfij	Relevance /weight 1 to 4 w(i,j)	Code question	evaluation 1 to 4	mean evaluation 1 to 4 eval(i,j)	Security factor score Sfis
Domain: Access control						
Sf20. Business requirements for access controlPremise	access control policymanagement	3	20.1	3	2,67	2,67
			20.2	3		
			20.3	2		
		3				
Sf21. User access management	registration of users	2	21.1	1	1	2,25
	privilege management	1	21.2	3	2	
			21.3	1		
	user password management	4	21.4	3	2	
			21.5	1		
	review of user access rights	3	21.6	4	3,5	
			21.7	3		
		10				

Sfis = sum [(w(i,j) * eval(i,j)] / sum w(i,j)

Figure 2: Calculation of the Sf i's

When the questionnaire is completed, BEVA now calculates the security factor scores (Sf) being:

Sfi s = sum [eval (i,j) * w(i,j)] / sum w(i,k)

If all the factor scores are calculated also a general security score Ss is given:

Ss= sum [eval (1,36) * w(1,36)] / sum w(1, 36)

For example see factor 21 in the example: Sf21:[2*1 + 1*2 + 4*2 + 3*3,5]/10 = 2.25

Ss= in this example 2.66

Security Factor	Weight	Sfi	Security Factor	Weight	Sfi
1	A	2,25	19	B	3,5
2	D	3,33	20	B	2,67
3	B	2,75	21	A	2,25
4	A	3	22	D	2
5	C	1,75	23	E	2,33
6	D	2,33	24	C	2
7	A	2,25	25	A	2,67
8	B	3,25	26	D	2,5
9	E	2,33	27	B	1,75
10	D	2,67	28	E	3
11	C	2	29	B	3,25
12	A	3,67	30	C	3,33
13	C	3	31	B	2,75
14	B	2,5	32	C	2,67
15	D	1,67	33	A	2
16	A	2,67	34	E	2
17	E	3,33	35	C	2,5
18	C	2,25	36	B	3

Figure 3: Sfi's results

Based on the evaluated questionnaire and the allocated weights, a realistic picture of the security situation of the company can be created as well general as by factor. The system BEVA creates a graphical output of the correlation diagram between these two variables measured for all aspects. Figure 4 shows the scores of all the security factors.

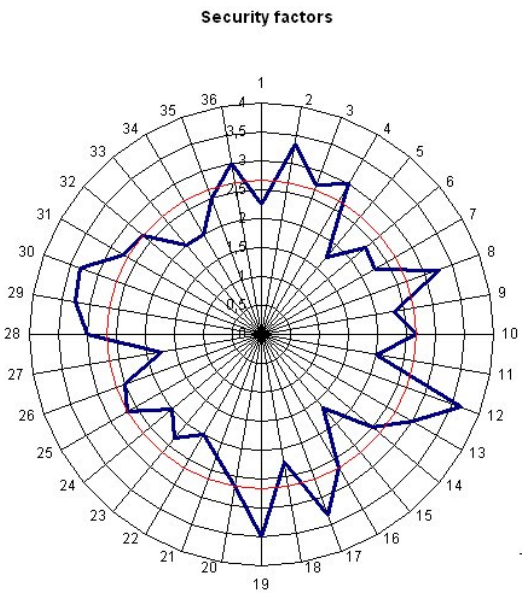


Figure 4: Graph of the security scores

The red line states Ss the general security score. The blue line connects the individual scores of the security factors. Security factors 1, 5, 6, 7, 9, 11, 14, 15, 18, 21, 22, 24, 26, 27, 33 and 34 score beneath the general security score.

Figure 5 combines the scores of the security factor with its importance. For example factor 33 scores low namely 2 but has importance A, low importance. Factor 34 scores also 2 but had importance E, high importance.

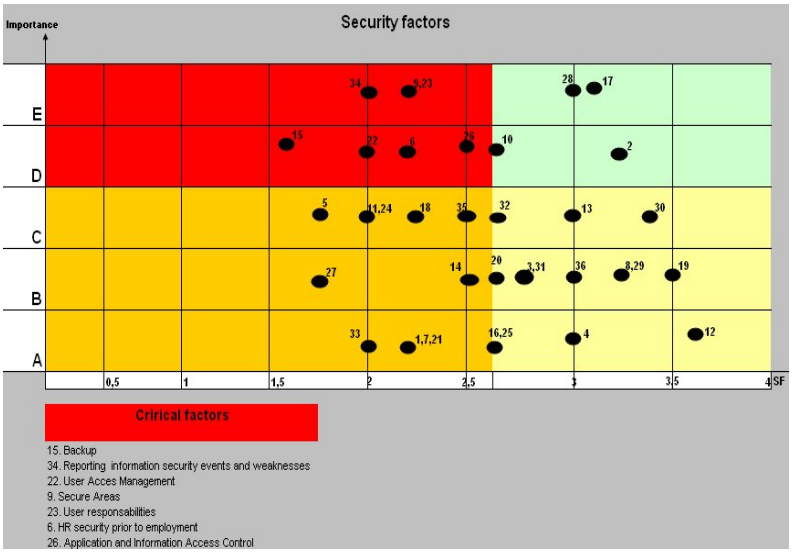
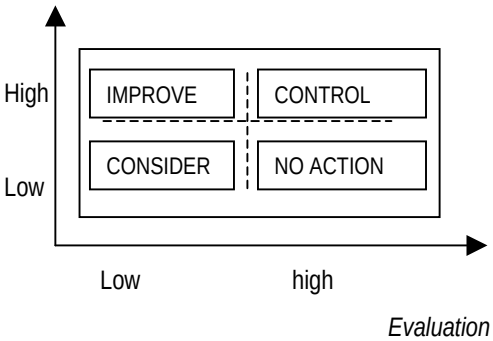


Figure 5: Graph of security factors and their importance

These differences are well stressed in this graphic. As you can see the ***red*** area highlights the security factors that score low and have a high importance. The factors lying in this area are critical and need immediate attention.

The ***green*** area is important and good secured. It is important to continue these actions and follow up these factors well. The *yellow* zone scores good but isn't that important, no action needs to be taken here. The less important factors that don't score well are situated in the *orange* zone. These factors need to be considered but probably with a small piece of the budget.

Importance/relevance



Now a clear view of the security situation is obtained. Feedback is given to the company and the evaluation states immediate points of action.

3. The occurrence of threats

The yearly organised CSI/FBI-study delivers the following probabilities for the threats:

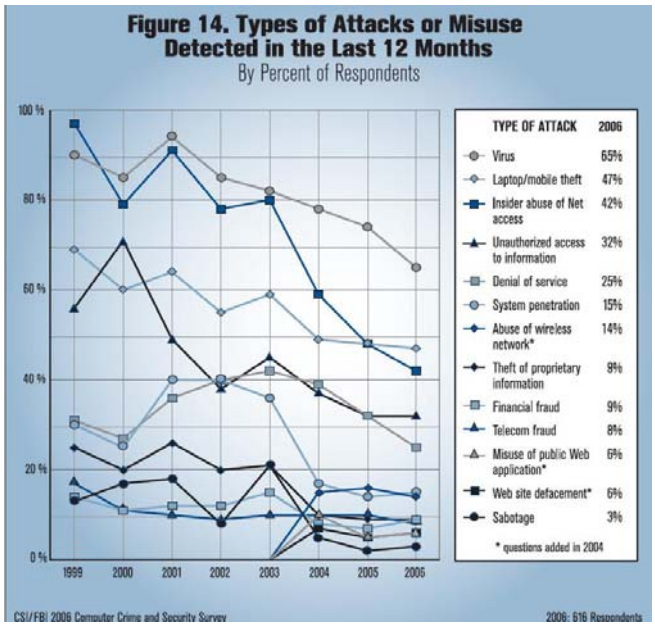


Figure 6: Threats and their occurance

Our final goal is to influence the occurrence of the threats, or the probability of the occurrence of them, by implementing selective security measures in the company. This will impact in the long run the security situation.

We must concentrate on the critical security factors, following the results of the audit. If the security factor is critical, than the threats linked with it have a critical risk too.

In figure 7 we figure out the relations between the threats and the security factors.

		1.1 Informatie-beveiliging als aspect van continuity management	2.1 Vereisten voor toegangs-controle	2.2 Management van gebruikers-toegang	2.3 Gebruikers-verant-woordelijkheid	2.4 Controle netwerktoegang	2.5 Controle op toegang tot OS	2.6 Toegangs-controle op applicaties en informatie	2.7 Gebruik van mobiele infrastructuur	3.1 Beveiligings-vereisten voor systemen
Kans / Dst / **Bedreiging**		2,38	2,33	2,46	2,83	2,76	2,90	2,60	2,96	3,0
Virus	0,65									
Diefstal van Laptop/mobiel apparaat	0,47								1	
Misbruik van netwerktoegang door interne gebruikers	0,42					1				
Ongeauthoriseerde toegang tot informatie	0,32		1	1	1					
Denial of Service - aanval	0,25	1								
Systeem inbraak/systeem penetratie	0,15		1	1	1					
Misbruik draadloos netwerk	0,14		1	1		1			1	
Diefstal van cruciale data	0,09		1	1						
Financiële fraude	0,09			1		1				
Fraude met telecommunicatie	0,08								1	
Misbruik van publieke Web-applicaties	0,06							1		
Website-defacement	0,06		1	1						
Sabotage aan data of netwerapparatuur	0,03	1					1			
Illegale software applicaties op het systeem (bots, trojan horses...)	0,03									
Phishing waardoor de organisatie als afzender werd voorgesteld maar dit niet was	0,03									
Misbruik door chattende	0,03									

Figure 7: relation threats and security factors

3. Security measures and follow up

A next step is to create a list of action points. Taking into account the stated security budget and the factors and their importance, an action plan is suggested.

First a table wit the most used measures along the CSI-study.

Most used measures (CSI-study)
Firewall
AntiVirus Software
AtiSpyware Software
Server Based Acces control list
Intrusion detection system
Ecryption for data
Reusable account system
Intrusion prevention system
Log management software
Application level firewall
Smart card/one time password token
Specialized wireless security
Training personel
Endpoint security client software
Update server
Firewall
AntiVirus Software
AtiSpyware Software
Server Based Acces control list
Intrusion detection system

Figure 11: Most used measures

Next a fraction of the table which states the relation between the measures and the threats is given.

Bedreigingen / Maatregelen	Virus	Diefstal van Laptop/mobiel apparaat	Misbruik van netwerktoegang door interne gebruikers	Ongeautho riseerde toegang tot informatie	Denial of Service - aanval	Systeem inbraak/systeem penetratie	Misbruik draadloos netwerk	Diefstal van cruciale data	Financiële fraude	Fraude met telecommunicatie	Misbruik van publieke Web-applicaties	Website-defacement	Sabot aan d of netwe aratu
Firewall	0	0	0	1	1	1	0	0	0	0	1	1	
AntiVirus Software	1	0	0	0	0	0	0	0	0	0	0	0	
AtiSpyware Software	0	0	0	0	0	0	0	0	0	0	0	0	
Server Based Acces control list	0	0	0	1	0	1	0	1	0	0	0	0	
Intrusion detection system	0	0	0	1	0	1	0	1	0	0	1	1	
Ecryption for data	0	0	0	1	0	0	0	1	0	0	0	0	
Reusable account system	0	0	0		0	0	0	0	0	0	0	0	

Figure 8: relation measures and threats

The action plan concerning security will be implemented, taking into account the weakest security factors and of course considering the budget.

After a period of approximately 3 months after implementing the security measures, a new security audit should be taken. The new security score Ss is calculated and compared to the stated aimed Security score using the security measures. If there are security factors that score too low, these should be investigated and adjusted.

Conclusion

The awareness that security is a management problem is everywhere present. It's critical to know what are the critical resources and processes of the company and their weaknesses. Our security audit is a handy solution. We have developed BEVA, a method to critically analyse the company and to uncover the weak spots in the security system. BEVA results in security scores for each security factor and also in a general security score. The goal is to increase the security score Ss to a postulated level by focusing on the critical security factors, those with a low security score. The results of the audit are an ideal start to do risk analysis.

Bibliography

[Shannon, 1949] C.E.Shannon. The Mathematical theory of communication. In: The Mathematical Theory of Communication. Ed. C.E.Shannon and W.Weaver. University of Illinois Press, Urbana, 1949.

[Jean-Marc Lamère] la sécurité informatique; Dunod : La méthode MARION (Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux) www.eisti.fr/~bg/COURSITACT/TXT/m_marion.txt

[Val Thiagarajan B.E,2005] Information Security Management ; BS ISO/ IEC 17799:2005 ; SANS Audit Check List: author:., M.Comp, CCSE, MCSE, SFS, ITS 2319, IT Security Specialist.

(www.riskworld.net/7799-2.htm)

[Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn and Robert Richardson] 2006 CSI/FBI-study about cybercrime: COMPUTER CRIME AND SECURITY SURVEY

https://event.on24.com/eventRegistration/EventLobbyServlet?target=registration.jsp&eventid=27372&sessionid=1&key=42F39B89EE0B30BA951711A5E7A98EDD&sourcepage=register

http://mediaproducts.gartner.com/gc/webletter/computerassociates/vol3issue3_risk/index.html

Security Management: A New Model to Align Security With Business Needs; Sumner Blount, CA Security Solutions ;August 2006

Authors' Information

Jeanne Schreurs – prof. Business informatics, Universiteit Hasselt; gebouw D, Agoralaan, 3590 Diepenbeek, Belgium; e-mail: jeanne.schreurs@uhasselt.be

Rachel Moreau - Universiteit Hasselt; gebouw D, Agoralaan, 3590 Diepenbeek, Belgium; e-mail: Rachel.moreau@uhasselt.be