D. Vorobey, Master student
I. Sugoniak, PhD, As. Prof.
V. Shadura, senior teacher, language advisor
Zhytomyr State Technological University

THREAT ANALYSIS OF COMPUTER FILE-SERVER USING EXPERTS' EVALUATION METHOD

Nowadays, the majority of companies and educational establishments have file-servers at their disposal. The company's success and the confidentiality data provision are affected by the efficiency of these servers. Files of any extension could be stored on them while the access is available for authorized people twenty four hours a day.

File-server is represented by a dedicated server designed for execution of input/output data operations. As a rule, file-server has a big size of disk space, negotiated in form of RAID-array to provide trouble-free and enhanced data reading and writing speed. The advantages are the law cost and short development time, software update and upgrade. The main disadvantage is the low level of the system security.

Thus, 8 highly qualified specialists in information security were selected to evaluate the threat level. While designing the questionnaires they defined what exactly, in their opinion, could cause the biggest damage, namely:

- «Hackers' attacks» are the actions of cyber criminals, which are aimed at information capture from fileserver or gaining control over it or breaking its systems down;
- «Virus upload» are the intentional or unintentional infecting the server with viruses, which are aimed at data destroying;
- «Hardware failures» are the power surge, wear and tear details, loosen hookups, etc;
- «Software failures» is the overload, bugging, software aging, etc;
- «Theft» is server stealing or the whole information stealing remotely or direct copying;
- «Targeted download information» is committed to satisfy a cyber criminal interests or to find information about competitors;
- «Negligence» is a non-execution or unduly execution of server maintenance as a result of careless attitude to work;
- «Sabotage» is a purposeful breakdown of the server operation as a result of careless execution of duties;
- «Accidents» are the war, accidental physical impact on the server, a spilt cup of coffee, natural disasters such as fire, typhoon, flood, earthquake, etc;
- «Purposeful information deleting» is a situation which can occur, for example, at a University in case a competitor has bribed an employee of our University in order not to let other students take part in the competition.

By using the proposed list of threats the experts defined those, which are the most dangerous and the least damage causing. The total expert responses were defined on irregularity by means (the means of Ms Excel spreadsheet). It is possible to find information about threats which are of higher importance using «SUM» and «STDEVIATION» (table1).

Table 2

Computer file-server threat rating

		Threat name	Number of points
1	1	Hackers' attacks	69
2	2	Accidents	62
3	3	Virus upload	60
4	4	Software failures	49
	5	Hardware failures	40
5	6	Theft	30
6	7	Targeted download information	28
	8	Purposeful information deleting	17
7	9	Sabotage	14
8	10	Negligence	9

9	Accidents	62	7,75	0,707106781	0,091239585
10	Purposeful information deleting	17	2,125	0,640869944	0,301585856

According to the calculation results it can be found out the computer file-server threat rating (table 2).

Thus, the experts concluded, that the «Hackers' attacks» could cause the greatest damage and «Negligence» could cause the least one.

The standard deviation, which is defined with the help of «STDEV» function and variability coefficient, is shown in table 1. While, the closer to 0 is the standard deviation value, the smaller is the difference between standard experts' deviation value and the average value. The variability value is less than 0,33 , therefore the variability is small. Therefore, the comparability of the experts' thoughts about the investigated process has to be taken into account.

Let us look at how experts' opinion can be compared. Since we have more than two rated attributes, so to evaluate the experts' concord, the concord coefficient will be used.

Let us use the formula:

$W = \left(\sum_{j=1}^{n} d_j^2\right) / m^2(n^3 - n)$; and $d_j = S_j - \frac{1}{n}\sum_{j=1}^{n} S_j$; n number of factors, m is the number of experts, d_j is the deviation sum of the average sum, S_j is the sum of ranks.

We have W = 0,789318. W is closer to 1 coefficient, the bigger is comparability among the experts' thoughts. As usual, the experts' opinions are believed to be agreed if this value is 0,7 or higher. Consequently, the opinions of our experts are in agreement.

Meanwhile, the concord coefficient has been calculated in order to be checked for static significance. So the number of potential risks is more than 7 (we have 10), that is why it is to be checked for static significance applying Pearson criterion $X^2_{розрах}$= 22,1. But the table value is = 14,1 by significance level a $X^2_{табл}$ = 0,05 and degree of freedom.

Thus, according to the results obtained, the concord coefficient is more than 0,7 and the value of Pearson criteria is bigger than in the table one, therefore, experts' opinion is fully agreed.

Now than, with the help of experts' evaluation method, the computer file-server threats are rated and the results are checked. Hacker attacks, accidents, virus upload, software failures, hardware failures, theft, targeted download information, purposeful information deleting, sabotage, negligence are the main threats by their harmful effect.