Combining technical and financial impacts for countermeasure selection

Gustavo Daniel Gonzalez Granadillo, Christophe Ponchel, Gregory Blanc, Hervé Debar

Combining Technical and Financial Impacts for Countermeasure Selection

Gustavo Gonzalez-Granadillo
Institut Mines-Télécom, Télécom SudParis, CNRS UMR 5157 SAMOVAR
9 rue Charles Fourier, 91011 Evry, France
gustavo.gonzalez_granadillo@telecom-sudparis.eu

Christophe Ponchel
Cassidian CyberSecurity
1 bd Jean Moulin, 78996 Elancourt Cedex, France
christophe.ponchel@cassidian.com

Gregory Blanc
Institut Mines-Télécom, Télécom SudParis, CNRS UMR 5157 SAMOVAR
9 rue Charles Fourier, 91011 Evry, France
gregory.blanc@telecom-sudparis.eu

Hervé Debar
Institut Mines-Télécom, Télécom SudParis, CNRS UMR 5157 SAMOVAR
9 rue Charles Fourier, 91011 Evry, France
herve.debar@telecom-sudparis.eu

Research in information security has generally focused on providing a comprehensive interpretation of threats, vulnerabilities, and attacks, in particular to evaluate their danger and prioritize responses accordingly. Most of the current approaches propose advanced techniques to detect intrusions and complex attacks but few of these approaches propose well defined methodologies to react against a given attack. In this paper, we propose a novel and systematic method to select security countermeasures from a pool of candidates, by ranking them based on the technical and financial impact associated to each alternative. The method includes industrial evaluation and simulations of the impact associated to a given security measure which allows to compute the return on response investment for different candidates. A simple case study is proposed at the end of the paper to show the applicability of the model.

Keywords. Cyber Protection Level, Countermeasure Selection, Complex Attacks, Security Metrics, Decision Support.

1 Introduction

Innovation in Information Technology has brought numerous advancements but also some consequences. Cyber attacks have evolved along with technology, reaching a state of high efficiency and performance. Current research focuses on approaches to detect such attacks and demonstrate their strengths and the difficulty to mitigate them [1, 2]. Most of these works propose approaches to detect complex attacks but few of them propose a methodology to react against them.

In addition, research in dynamic response proposes automatic response mechanisms (e.g., the adaptation of security policies) to overcome the limitations of manual responses. However, these approaches

J. Garcia-Alfaro, G. Gür (Eds.): Advanced
Intrusion and Prevention Workshop 2014 (AIDP 2014)
EPTCS 165, 2014, pp. 1–14, doi:10.4204/EPTCS.165.1

remain limited since they do not analyse the impact of the selected countermeasures [3]. Inappropriate selection of countermeasures result in disastrous consequences for the organisation. An impact analysis of all the security candidates is therefore essential in the decision process to select appropriate countermeasures for a given attack.

In this paper, we propose a novel and systematic method to select security countermeasures from a pool of candidates, by ranking them based on the trade-off between their efficiency in stopping the attack, and their ability to preserve, at the same time, the best service to legitimate users. The method includes industrial evaluation and simulations of the impact associated to a given security measure.

The rest of the paper is structured as follows: Section 2 introduces the state of the art on service protection level, and return on response investment. Section 3 presents the security and financial countermeasure impact analysis. Section 4 details the quantification of the proposed countermeasure impact model. Section 5 gives an example of a case study. Finally, conclusions and perspectives for future work are presented in Section 6.

2 State of the Art

2.1 Cyber Protection Level

The cyber protection level is an evolution of the safety integrity level (SIL) [4, 5], which is defined as a relative level of risk reduction provided by a safety function. A SIL is determined based on a number of quantitative factors (using methods such as: risk matrices, risk graphs, layers of protection analysis) in combination with qualitative factors such as development process and safety life cycle management.

The cyber protection level refers to the strength of cyber security means deployed against a particular threat. The process is generally used to identify assets, threats, vulnerabilities, likelihood, countermeasures, and consequences. This is usually obtained from a risk analysis, following any of the international standards (e.g., NIST [6], ISO [7]), or any of the risk management methodologies (e.g., MEHARI [8] and EBIOS [9]) as well as expert knowledge. In our study, we consider the EBIOS methodology, defined by the French National Security Agency (ANSSI)[9].

The analysis follows several steps: 1) the context definition that determines stakeholders, processes, assets and dependencies, threat sources and existing security; 2) feared events and threat scenarios, with impact and occurrence probability; 3) risk evaluation that takes into account the existing security described in (1); 4) necessary measures related to risk mitigation.

Although most organizations follow a particular methodology to deploy a risk analysis, current approaches present several shortcomings: they rarely propose calculation methods for the protection level; none of them can be applied on an operational environment with “living” protection means (i.e., potentially unavailable for a period of time); they do not consider the different instances that must be deployed in the network to cover the threat everywhere; the effectiveness of a protection function is hardly considered in the analysis.

2.2 Cost Sensitive Metrics

Cost sensitive metrics are widely proposed as a viable approach to find an optimal balance between intrusion damages and response costs, and to guarantee the choice of the most appropriate response without sacrificing the system functionalities.

2.2.1 Return On Investment (ROI):

The simplest and most used approach for evaluating financial consequences of business investments, decisions and/or actions is the ROI metric. ROI is a relative measure that compares the benefits versus the costs obtained for a given investment [10, 11].

ROI basically shows how much a company earns from invested money. This metric supports decision makers in selecting the option(s) that have the highest return. ROI is calculated as the present value of accumulated net benefits over a certain time period minus the initial costs of investment, then divided by the initial costs of investment, as shown in Equation 1.

$$ROI = \frac{B_t - C_t}{C_t} \times 100 \tag{1}$$

Where:
B_t refers to all benefits during period t,
C_t refers to all costs during period t

The decision rule is that the higher the ROI value, the more interesting the investment. However, Jeffery [10] agrees that the major problem with ROI is that the metric does not include the time value of money, i.e., a 100% ROI realized 1 year from today is more valuable than a 100% ROI realized over 5 years. Furthermore, the costs and benefits of the project may vary over time, meaning that the cash flows are different in each time period. As a result, ROI is not a convenient way to compare projects when the costs and benefits vary with time, and it is also not useful for comparing projects that will run over different periods of time.

2.2.2 Return On Security Investment (ROSI):

It is a relative metric that compares the differences between the damages caused by attacks (before and after countermeasures) against the cost of the countermeasure [12, 14, 13]. To calculate ROSI, a formula adapted from the ROI metric is presented in Equation 2.

$$ROSI = \frac{(ALE_b - ALE_a) - Cost_{CM}}{Cost_{CM}} \times 100 \tag{2}$$

Where:
ALE_b refers to the annual loss expectancy before countermeasure,
ALE_a refers to the annual loss expectancy after countermeasure,
$Cost_{CM}$ is the cost of the countermeasure

The calculation of each parameter composing the ROSI equation has been widely discussed by Lockstep Consulting [12], and Kosutic [13]. The former proposes a methodology that considers different levels of likelihood and severity, which are then, respectively transformed into frequency and direct cost; the latter considers on the one hand, parameters associated to the incident (e.g., financial losses, costs, frequency), and on the other hand, parameters associated to the protection (e.g., cost, benefits, life expectancy of the security measure).

Similar to the ROI metric, the decision rule states that the higher the ROSI value, the more interesting the investment.

2.2.3 Return On Response Investment (RORI):

It is a service dependency index for cost sensitive response based on a financial comparison of the response alternatives [15]. RORI is an adaptation of the ROSI index [14] that provides a qualitative comparison of response candidates against an intrusion. RORI considers not only response effects on intrusions, but also response collateral damages as depicted in Equation 3.

$$RORI = \frac{[IC_b - RC] - OC}{CD + OC} \times 100 \tag{3}$$

Where:
IC_b represents intrusion impacts when no response is enforced,
RC refers to the combined impact of intrusion and response,
OC are operational costs that cover low level investments such as response setup and deployment costs
CD refers to collateral damages, which are costs that are added by a new response, and are not related to intrusion costs

The deployment of the RORI index into real world scenarios has presented the following shortcomings:

- The RORI index is not defined when no countermeasure is selected. Since the operational cost (OC) is associated to the security measure, the RORI index will lead to an indeterminacy when no solution is enforced (NOOP).
- The RORI index is not normalized with respect to the size and complexity of the infrastructure.
- The absolute value of parameters such as IC_b and RC is difficult to estimate, whereas a ratio of these parameters is easier to determine, which in turn reduces errors of magnitude [16].

3 Countermeasure Impact Analysis

3.1 Security Impact

Taking into account current shortcomings in risk analysis methodologies, we propose to evaluate a protection level against a threat, related to confidentiality, integrity, and availability, that considers technical ans business services as assets.

The protection level (PL) of a service S_i against a threat T_k is calculated using Equation 4.

$$PL(S_i, T_k) = 100 - max(0, AD - AP) \tag{4}$$

Where:

- AD = Assessed Danger, which represents the threat dangerousness in terms of confidentiality, integrity and availability (i.e., d_{Ck}, d_{Ik}, d_{Ak}), as well as the service value in terms of confidentiality, integrity and availability (i.e., v_{Ci}, v_{Ii}, v_{Ai}), as shown in Equation 5.

$$AD = \frac{(d_{Ck} \times v_{Ci}) + (d_{Ik} \times v_{Ii}) + (d_{Ak} \times v_{Ai})}{75} \times 100 \tag{5}$$

From Equation 5, $d_{Ck} \times v_{Ci}$ represents the confidentiality-related impact, $d_{Ik} \times v_{Ii}$ represents the integrity-related impact, and $d_{Ak} \times v_{Ai}$ represents the availability-related impact. The more dangerous the threat and/or the more important the service in terms of confidentiality, integrity, and

availability, the higher the impact. Values of dangerousness d and service v range from 0 to 5, therefore, the maximum possible value for AD is 75. We multiply this result by 100/75 in order to get homogeneous values of protection (assessed in a scale from 0 to 100).

The current proposal only considers the CIA services (i.e., confidentiality, integrity, and availability) for the calculation of the assessed danger, mainly due to two reasons: firstly, because the data is considered by the EBIOS methodology, and secondly, because the approach is used by our industrial partners at Cassidian Cybersecurity. However, it is also possible to use other parameters (e.g., criticality, accessibility, recuperability, vulnerability) as long as we are able to estimate their values for the selected threats and services.

- AP = Assessed Protection, which represents the protection assigned against the threat k for the service i (i.e., p_{ik}), as well as the effectiveness of the protection assigned against the threat k for the service i (i.e., e_{ik}), as shown in Equation 6.

$$AP = e_{ik} \times p_{ik} \tag{6}$$

From Equation 6, the assessed protection is estimated by experts. The effectiveness factor e_{ik} is calculated depending on the type and distribution of protection (e.g., false positive rates, coverage of the network, feedback from operational teams, subjective figure).

To measure the impact of changes on security (SI, for Security Impact), we compare current and potential situations as depicted in Equations 7 and 8

$$SI = PL_{potential}(S_i, T_k) - PL_{current}(S_i, T_k) \tag{7}$$

Where,

- $PL_{potential}$ is the protection level with a modified protection capacity against the threat T_k.

Equation 8 provides more details about the delta between the current and the potential situation.

$$\begin{aligned} SI = \quad & max\left(0, \left[\frac{(d_{Ck}\times v_{Ci})+(d_{Ik}\times v_{Ii})+(d_{Ak}\times v_{Ai})}{75} \times 100\right] - e_{ik} \times p_{ik}\right) - \\ & max\left(0, \left[\frac{(d_{Ck}\times v_{Ci})+(d_{Ik}\times v_{Ii})+(d_{Ak}\times v_{Ai})}{75} \times 100\right] - e'_{ik} \times p'_{ik}\right) \end{aligned} \tag{8}$$

The variation is being on the protection p_{ik} and/or its effectiveness e_{ik}.

3.2 Financial Impact

An improvement of the RORI index has been proposed, taking into account not only the countermeasure cost and its associated risk mitigation, but also the infrastructure value and the expected losses that may occur as a consequence of an intrusion or attack [16].

The improved RORI index handles the choice of applying no countermeasure to compare with the results obtained by the implementation of security solutions (individuals and/or combined countermeasures), and provides a response that is relative to the size of the infrastructure. The improved Return on Response Investment (RORI) index is calculated according to Equation 9.

$$RORI = \frac{(ALE \times RM) - ARC}{ARC + AIV} \times 100 \tag{9}$$

Where:

- ALE is the Annual Loss Expectancy and refers to the impact cost obtained in the absence of security measures. ALE is expressed in currency per year (e.g., $/year) and and includes loss of assets (La), loss of data (Ld), loss of reputation (Lr), legal procedures (Lp), loss of revenues from existing clients or customers (Lrec), loss of revenue from potential clients (Lrpc), other losses (Ol), contracted insurance (Ci), and the annual rate of occurrence (ARO), i.e., $ALE = (La + Ld + Lr + Lp + Lerc + Lrpc + Ol - Ci) \times ARO$

- RM refers to the Risk Mitigation level associated to a particular solution. RM is defined from the security impact as a percentage (i.e., $0\% \leq \text{RM} \leq 100\%$) that represents the additional countermeasure effectiveness over the best solution to be implemented in order to totally eradicate the threat. RM includes the protection level of potential and current situations, as presented in Section 3.1 (i.e., RM = $\frac{PL_{potential}(S_i,T_k) - PL_{current}(S_i,T_k)}{100 - PL_{current}(S_i,T_k)}$)

- ARC is the Annual Response Cost that is incurred by implementing a new security action. ARC = OC+CD from Equation 3. ARC is always greater than or equal to zero ($ARC \geq 0$), and it is expressed in currency per year (e.g., $/year). ARC includes Direct costs: e.g., Cost of implementation (Ci), Cost of maintenance (Cm), Other direct costs (Odc); and Indirect costs (Ic), i.e., $ARC = Ci + Cm + Odc + Ic$

- AIV is the Annual Infrastructure Value (e.g., cost of equipment, services for regular operations) that is expected for the system, regardless of the implemented countermeasures. AIV is greater than zero ($AIV > 0$), and it is expressed in currency per year (e.g., $/year). AIV includes the following costs: Equipment Costs (Ec), Personnel costs (Pc), Service costs (Sc), Other costs (Oc), and Resell Value (Rv), i.e., $AIV = Ec + Pc + Sc + Oc - Rv$

4 Countermeasure Impact Quantification

The quantification of the parameters composing the RORI model proposed in Equation 9 is a task that requires expert knowledge, statistical data, simulation and risk assessment tools. Our experience in quantifying impact losses, as well as countermeasure costs and benefits for different security systems demonstrate that within 3 to 4 hours of discussions with use case providers and simple simulation runs, we are able to estimate each parameter composing the RORI model. The remaining of this section proposes a simple and well structured methodology to help security analysts in the estimation of such parameters.

4.1 Annual Loss Expectancy

For the estimation of the ALE, we adopted the approach proposed by Lockstep [12] to use the severity scale of values, which convert qualitative estimations into quantitative values of costs. For instance, a ‘minor’ loss of assets (La) represents a cost of $1,000; whereas a ‘serious’ loss of assets (La) represents a cost of $1,000,000. The estimation of all other losses (i.e., Ld, Lr, Lp, Lrec, Lrpc, Ol) follows the same approach.

The likelihood of an incident is transformed into a frequency value, which results into the Annual Rate of Occurrence (ARO) parameter. For instance, a ‘low likelihood’ means that the incident is likely

to occur once every year, (ARO = 1); whereas, a 'high likelihood' means that the incident is likely to occur once per month or less, (ARO = 12).

Both parameters (i.e., severity and likelihood) are estimated using a survey and scoring system, which combine expert knowledge and statistical data to quantify risk exposure. In order to handle uncertainty, we use Monte Carlo simulation. To run our simulation, we chose triangular distributions to evaluate the most likely values assigned to each level of security and likelihood, with minimum and maximum possible values of each level. This type of statistical computations can be easily achieved using basic statistical software or spreadsheet editors[1][2].

After 250 iterations, we were able to obtain a value of the losses and frequency that compose the ALE parameter, which represents the expected annual loss as a consequence of the realization of a given threat.

4.2 Risk Mitigation

A risk analysis, as performed by Cassidian cyber-security experts[3], gives the list of threats directly endangering business and technical services of the entity to protect, and the available protection means. The level of protection related to a given set of services is assessed using different kinds of information:

1. Types of security devices able to detect and/or react against an activity related to a threat occurrence; given by cyber-security experts.
2. Instances of security devices actually deployed to protect services; given by security architects

Services are modelled using dependency models. Identified threats and related protection measures (if they exist) are associated to services. We obtain, for each service a list of couples (threat, protection).

A threat is characterized by a dangerousness level in terms of confidentiality (i.e., d_{Ck}), integrity (i.e., d_{Ik}) and availability (i.e., d_{Ak}). We consider each service and their value as per confidentiality (i.e., v_{Ci}), integrity (i.e., v_{Ii}) and availability (i.e., v_{Ai}) in order to determine the potential effect of threats on services. An example of the asset values is represented in Table 1.

Dangerousness levels and values are integers ranging from 0 (meaning respectively no danger / no value) to 5 (meaning respectively highest danger / biggest value). Dangerousness and asset values are given by experts. Cell values are calculated using the AD such as described in Equation 5. Highest threat effect would be 75 (dot product of danger level and service value per CIA criteria). The result is finally reported as a percentage. It is important to note that the "N/A" flag in some cells means the threat does not endanger the service.

A protection (p_{ik}) is characterized by its effectiveness (e_{ik}) to prevent a threat from occurring. This is an integer ranging from 0 to 100. The protection either exists ($p_{ik} = 1$) or does not exist ($p_{ik} = 0$). When the protection is different from 0, the related threats are supposed to be mitigated by some of the protection means described in the service model.

Table 2 depicts an example of protection capacity on different services affected by several threats. We identify the services at which protection measures have been deployed, and their ability to mitigate threats. As a result, we consider the actual danger being the difference of threat level and protection level. Results of the aforementioned example are depicted in Table 3.

[1] Quadrant: The Quick and dirty risk analysis tool, available at: www.qdrnt.com/home.htm

[2] Monte Carlo simulation for excel featuring distribution strings, available at: http://xlsim.com/xlsim/index.html

[3] http://www.cassidiancybersecurity.com/en_US/web/guest/cybersecurity

Table 1: Assessed Dangerousness Matrix

			C	5	5	0	4	3
			I	5	5	0	4	3
			A	5	5	2	4	3
C	I	A		Service1	Service2	Service3	Service4	Service5
1	2	3	Threat1	40	40	8	32	24
3	3	3	Threat2	60	60	N/A	N/A	N/A
2	2	2	Threat3	N/A	N/A	5	32	24
5	5	5	Threat4	N/A	100	N/A	N/A	N/A
4	4	4	Threat5	N/A	N/A	N/A	N/A	48
5	5	5	Threat6	100	100	13	80	60
3	3	3	Threat7	60	60	8	36	36
2	2	0	Threat8	N/A	27	0	N/A	N/A
4	5	3	Threat9	80	N/A	N/A	N/A	N/A
3	3	3	Threat10	60	60	8	48	36

Table 2: Protection Capacity

	Service1	Service2	Service3	Service4	Service5
Threat1					
Threat2	75	75			
Threat3			60	60	60
Threat4					
Threat5					40
Threat6	100	100	100	100	100
Threat7	50		50		50
Threat8					
Threat9					
Threat10	90	90	90	90	90

Table 3: Actual Danger Matrix

			C	5	5	0	4	3
			I	5	5	0	4	3
			A	5	5	2	4	3
C	I	A		Service1	Service2	Service3	Service4	Service5
1	2	3	Threat1	40	40	8	32	24
3	3	3	Threat2	-15	-15	N/A	N/A	N/A
2	2	2	Threat3	N/A	N/A	-55	-28	-36
5	5	5	Threat4	N/A	100	N/A	N/A	N/A
4	4	4	Threat5	N/A	N/A	N/A	N/A	8
5	5	5	Threat6	0	0	-87	-20	-40
3	3	3	Threat7	10	60	-42	36	-14
2	2	0	Threat8	N/A	27	0	N/A	N/A
4	5	3	Threat9	80	N/A	N/A	N/A	N/A
3	3	3	Threat10	-30	-30	-82	-42	-54

Empty cells from Table 2 mean that protection does not exist in such service against a particular threat. Cells from Table 3 show the actual danger. In order to obtain the PL value in each cell, we use Equation 4

4.3 Annual Response Cost

In contrast to the AIV parameter, the ARC is a variable cost associated with the implementation of a given countermeasure. For instance, let us suppose that the user authentication information of a Web service is stored in a database. Whenever users want to access the system, they need to provide their corresponding login and password. However, for suspicious users, the organization wants to implement a countermeasure that asks for a double authentication (e.g., a challenge question, a security pin). The implementation of this countermeasure requires the organization to spend additional employee-hours which in turn represents a given cost. This latter is defined as the cost of implementation (Ci).

In addition, the countermeasure is going to be active only for suspicious users for a given period of time, which means that the system will turn the countermeasure from 'on' to 'off' according to the security tests and analysis performed. These tests and analysis represent the cost of maintenance (Cm) to the organization.

The activation/deactivation of a given countermeasure engenders other direct and indirect costs. For instance, requesting an additional authentication method to legitimate users may cause these users to unsubscribe from the service and search for another one. This collateral damage represents an indirect cost (Ic) to the organization. Collateral damages can be quantified as the variation between the current and the projected productivity that an organization experiences due to a side effect of a given solution [14].

4.4 Annual Infrastructure Value

This parameter is calculated as the sum of the annual value of all the equipments, i.e., Policy Enforcement Points (PEP), that are needed to be deployed in the preliminary phase of the system architecture in order to guarantee a desired level of security. The AIV includes the cost of purchasing, licensing, and/or leasing the security equipments in a given organization.

It is important, however, to answer the following questions while estimating the AIV parameter:

- What kind of PEPs (e.g., Firewalls, IPS, IDS, SIEM) and which quantity is required for the system security?
- What is the lifetime expectancy of the PEP?
- What is the PEP's deployment time?
- What is the annual cost of purchase, licensing or leasing of the PEP?
- How many employee-hours are required for the operation of the PEP?
- How long (i.e., hours/year) is the PEP expected to be active?
- Is there an insurance contracted for the PEP? If so, how much does it cost per year?
- How frequently (i.e., times/year) does the PEP need to be checked or maintained?
- Is there any other cost associated with the operation of the PEP in the security infrastructure?
- What is the amortization value of the PEP?

5 Use Case

This section describes a simple case study provided by Cassidian CyberSecurity, the cyber security company of the Airbus group, and a major provider of global security solutions and services.

The scenario is based on a risk analysis performed on a company, limited to three services. The security auditors have determined the value of these services for the company, taking into account the company activity, stakeholders, technical and human constraints (e.g., skill level of the personnel in terms of security-related good practices), the loss of money in case of failures, etc. The risk analysis has been performed according to the EBIOS methodology. Four threats have been considered in this study. Their effects on targeted elements enable the auditors to evaluate the dangerousness criteria. Countermeasures have been proposed by the auditors to make the risk level acceptable along the company criteria.

The subsequent deployment of security devices compliant with the experts recommendations leads to provide the following matrices : threat target matrix (Table 4), and protection capacity matrix (Table 5).

Table 4: Threat Target Matrix

			C	0	5	5
			I	5	5	5
			A	5	5	3
C	I	A		Web services	Network infrastructure	User service
1	3	2	Web site sabotage	33	N/A	N/A
3	1	5	Network infrastructure attack	N/A	60	N/A
5	4	2	User workstation compromise	N/A	N/A	68
5	4	3	Admin workstation compromise	N/A	N/A	72

Table 5: Protection Capacity Matrix

	Web services	Network infrastructure	User service
Web site sabotage	50		
Network infrastructure attack		80	
User workstation compromise			17
Admin workstation compromise			50

The main danger on user and admin workstations lies in their compromission by malware programs. To counter this threat we deploy a protection with an effectiveness assessed by experts e = 50%. The effectiveness value is obtained considering several criteria:

- reliability of the malware detection software: the cyber company leading audits maintain a knowledge base regarding the reliability of security products. Particularly, anti-virus system reliability has been tested against malwares discovered and published within a period of 6 months. These tests are possible using online services such as VirusTotal. With an up-to-date base, 80% of the injected malware programs were detected by the malware detection tool deployed in the audited company. Then reliability score is 80%.

- signature base update policy: the frequency is set to one per week, which is assessed being far from achieving complete protection, therefore the score is set to 60%. The following scale is being used: 100% daily update, 60 % weekly update, 20% monthly update, 5% annual update, 1% no update since installation.
- resilience : this one is 100%, as tests over a 1 month period do not reveal any dysfunction. Indeed the cyber security company periodically launches test campaigns on security product resilience.

The effectiveness is then evaluated as the product of the reliability, policy and resilience scores (i.e., e = reliability_score $\times$ update_policy_score $\times$ resilience_score). This gives a result of 48%, approximated to 50%. This kind of protection is deployed on every administration workstation, and in only 1/3 user workstations (900 PC among 2700 for the whole organization), mainly for cost reasons. The protection level (PL) is calculated using Equation 4, as follows:

PL (User service, User workstation compromise) = 100 - (68 - 17)

PL (User service, User workstation compromise) = 100 - 51 = 49

A malware is detected on a user computer (among those unprotected). The proposed countermeasure consists on deploying an anti-malware agent on it and extend the solution to the other 1,800 workstations. The technical assessment of the countermeasure is shown in Tables 6 and 7.

Table 6: Foreseen Protection Capacity Matrix

	Web services	Network infrastructure	User service
Web site sabotage	50		
Network infrastructure attack		80	
User workstation compromise			50
Admin workstation compromise			50

Table 7: Potential Danger Matrix

				Web services	Network infrastructure	User service
C				0	5	5
I				5	5	5
A				5	5	3
C	I	A				
1	3	2	Web site sabotage	-17	N/A	N/A
3	1	5	Network infrastructure attack	N/A	-20	N/A
5	4	2	User workstation compromise	N/A	N/A	18
5	4	3	Admin workstation compromise	N/A	N/A	22

The risk mitigation RM (user workstation compromise) = (82-49) / 51 = 65%. The anti-malware editor cost policy is the following: 40,000€ per year for a maximum of 2,000 embedded agents; 50,000€ per year for a maximum of 5,000 embedded agents.

Table 8: Countermeasure Evaluation against Malware Infection

Countermeasure	**ARC**	**RM**	**RORI**
C1. No operation (NOOP)	0 €	0.00	0.00%
C2. Install agent only in the infected hosts	17 €	0.01	1.31%
C3. Install agents in 1,100 hosts (to reach the 2000 agent-limit)	18,700 €	0.39	21.66%
C4. Install agents in 1,800 hosts (to protect all workstations)	40,600 €	0.65	21.11%

Considering that the annualized loss expectancy for a malware in the system is estimated at ALE = 100,000€ per year, and that the annual infrastructure value is estimated at AIV = 75,000€ per year, we use Equation 9 to perform the countermeasure evaluation. Table 8 shows these results, and details information regarding countermeasure cost, mitigation level, and RORI index.

From Table 8, the first candidate (i.e., C1) proposes to accept the risk by doing no operation (NOOP). This alternative does not provide any mitigation level (RM=0) and does not generate any additional cost (ARC=0). The expected return on the response investment is therefore null (RORI=0).

The second alternative (i.e., C2) proposes to install agents only in the infected host. This alternative will not change the danger of the total group of 2,700 hosts. The mitigation level will be therefore close to zero (RM=0.01). However, taking into account that a license to install an anti-malware agent for a maximum of 2,000 hosts is already being paid, the ARC value to be installed in 1 additional host will only consider the cost of deployment (e.g., deploying a license in one host takes in average 10 minutes, and 1 employee-hour costs 100€ at Cassidian Cyber Security), therefore ARC(1 host) = 17€.

The third alternative (i.e., C3) suggests to install agents in 1,100 additional workstations (the maximum number of hosts allowed by the license). The mitigation level is calculated considering the current protection level (*PLcurrent* = 49), and the potential protection level (*PLpotentiel* = 100- max (0, 68-50*2000/2700) = 69), therefore RM = (69 -49) / (100 -49) = 39%. In addition, the ARC for 1,100 additional hosts (to reach the 2,000 agents limit) is equivalent to ARC= 1100 x 17 = 18700 €. As a result, the return on response investment is equivalent to (RORI = 21.66%).

The fourth evaluated candidate proposes to install agents in every administration workstation of the whole organization (i.e., 2,700 workstations). This requires to pay an additional of 10,000€, for a license that will allow to install agents in a maximum of 5,000 hosts. The mitigation level is calculated considering the current protection level (*PLcurrent* = 49), and the potential protection level (*PLpotentiel* = 100- max (0, 68-50*2700/2700) = 82), therefore RM = (82 -49) / (100 -49) = 65%. In addition, the ARC for 1,800 additional hosts (to reach the 2,700 agents) is equivalent to ARC= 1800 x 17 = 30,600€+ 10,000€= 40,600€. As a result, the return on response investment is equivalent to (RORI = 21.11%).

After the evaluation of the different candidates to mitigate a malware infection, we select alternative 3 as the optimal countermeasure, since it provides the highest RORI index. C3 proposes to install anti-malware agents in 1,100 hosts, additional to the already 900 protected hosts.

6 Conclusions and Future Work

We have proposed in this paper a novel and well structured method to select security countermeasures from a pool of candidates, based on their technical and financial impact. The method includes industrial

evaluation and simulations of the impact associated to a given security measure.

By calculating the potential new protection level, we are able to compare the current versus the potential change. As a result, we obtain quantitative information on the improvement or degradation of security at the service level. However, nowadays this function is limited to the protection level measurement after the addition or removal of protection measures in the network (e.g., enabling/disabling a security function will be considered as an addition/removal security function). We do not support detailed settings of security devices such as filtering rules in a firewall.

Future work will define the full service protection level as the overall protection of services for the entity due to several reasons: 1) to be aware of the general security level; 2) because actions to improve security for a service may have negative consequences to others (e.g., move of a security device), or may decrease the protection against other threats (e.g., replacement of a security device).

Another task will consist in proposing guidelines for the protection effectiveness per type of security function. This parameter is very important in the proposed approach. Giving subjective value would ruin the effort to rationalize the RORI result.

Acknowledgements:

The research in this paper has received funding from the Information Technology for European Advancements (ITEA2) within the context of the ADAX Project (Attack Detection and Countermeasure Simulation)

References

[1] Agarwal, P., Efrat, A., Ganjugunte, S., Hay, D., Sankararaman, S., Zussman, G.: Network Vulnerability to Single, Multiple and Probabilistic Physical Attacks, Military Communications Conference, (2010), doi:10.1109/MILCOM.2010.5679556.

[2] Vetillard, E., Ferrari, A.: Combined Attacks and Countermeasures, International Federation for Information Processing, (2010), doi:10.1007/978-3-642-12510-2_10.

[3] Debar, H., Thomas, Y., Cuppens, F., Cuppens-Boulahia, N.: Enabling Automated Threat Response through the Use of a Dynamic Security Policy, Journal in Computer Virology, vol. 3, number 3, pp. 195–210, (2007), doi:10.1007/s11416-007-0039-z.

[4] Ingrey, A., Lereverent, P., Hildebrant, A.: Safety Integrity Level, Manual PEPPERL+FUCHS, (2007).

[5] Mitchel, M.: SIL Made Simple, White Paper presented at Valve World, (2010).

[6] National Institute of Standards and Technologies: Guide for Conducting Risk Assessment, (2012).

[7] International Standard ISO/IEC 27005: Information Technology - Security Techniques - Information Security Risk Management, (2008), available at `http://www.iso27001security.com/html/27005.html`.

[8] Clusif: MEHARI 2010 - Risk Analysis and Treatment Guide, (2010), available at `http://mehari.info/`.

[9] ANSSI: EBIOS 2010 - Expression of Needs and Identification of Security Objectives, (2010), available at `http://www.ssi.gouv.fr/IMG/pdf/EBIOS-1-GuideMethodologique-2010-01-25.pdf`.

[10] Jeffrey, M.: Return on Investment Analysis for e-Business Projects, Internet Encyclopedia, First Edition, Hossein Bidgoli Editor, vol. 3, pp. 211–236, (2004), doi:10.1002/047148296X.tie154.

[11] Schmidt, M.: Return on Investment (ROI): Meaning and Use, Encyclopedia of Business Terms and Methods (2011).

[12] Lockstep Consulting.: A Guide for Government Agencies Calculating Return on Security Investment, Available at: http://lockstep.com.au/library/return_on_investment, (2004)

[13] Kosutic, D.: Is it possible to calculate the Return on Security Investment (ROSI)?, Available at: http://blog.iso27001standard.com/2011/06/13/is-it-possible-to-calculate-the-return-on-security-investment-rosi/, (2011)

[14] Sonnenreich, W., Albanese, J., Stout, B.: Return On Security Investment (ROSI) – A Practical Quantitative Model, Journal of Research and Practice in Information Technology, vol. 38, number 1, (2006), doi:10.5220/0002580202390252.

[15] Kheir, N., Cuppens-Boulahia, N., Cuppens, F., Débar, H.: A Service Dependency Model for Cost-Sensitive Intrusion Response, Proceedings of the 15th European Symposium on Research in Computer Security (ESORICS), pp. 626–642, (2010), doi:10.1007/978-3-642-15497-3_38.

[16] Gonzalez Granadillo, G., Belhaouane, M., Debar, H., Jacob, G.: RORI-based countermeasure selection using the OrBAC formalism, International Journal of Information Security, Vol. 13(1), pp. 63–79, (2014), doi:10.1007/s10207-013-0207-8.