

脆弱性水平对信息系统安全技术策略影响研究

方玲*, 仲伟俊, 梅姝娥

(东南大学经济管理学院, 江苏南京 211100)

摘要: 利用博弈论研究了基于脆弱性水平的组织信息系统安全技术策略,发现信息系统脆弱性水平对组织信息系统安全技术的选择与配置具有重要影响.脆弱性水平较低时组织只需对一部分IDS警报事件发起人工调查,无须对未警报事件发起调查;脆弱性水平较高时组织需对所有IDS警报事件发起调查,同时还需对部分未警报事件发起调查.与此同时,人工调查率还将随着脆弱性水平的提高而提高.此外,当信息系统脆弱性水平比较高时,黑客入侵率不一定高,这主要是因为组织配置了入侵检测率较高的IDS.

关键词: 脆弱性水平;入侵检测系统配置;人工调查;信息系统安全;黑客成功率
中图分类号: C931.6;F272.3 **文献标识码:** A **doi:**10.7511/dllgxb201503016

0 引言

对信息系统安全来说,一种较为直接的保护方式就是尽可能减少信息系统脆弱性,因为脆弱性是黑客入侵信息系统成功的必要条件之一^[1-2].然而现实中几乎不存在零脆弱性的信息系统,信息系统安全工作者所能做的只是尽量减少系统脆弱性.减少信息系统脆弱性的方式主要有脆弱性扫描技术和补丁管理技术等,而这些技术都将为组织带来高昂的成本投入.另一种用于对付信息系统安全威胁的措施是部署若干信息系统安全技术,如防火墙、入侵检测系统(intrusion detection system,简称IDS)等.显然,组织所选用的信息系统安全技术组合首先应能处理或减轻其所面临的威胁;其次该安全技术组合应当具有最优配置,从而有利于组织最小化其安全防护成本并提高效率^[3-4].总的来说,第一种方式可降低系统脆弱性水平,第二种方式可降低黑客入侵率.许多组织在信息系统安全防护时都会同时使用这两种措施,而关键在于如何在这两种措施间寻找到平衡,从而使得组织在获得足够的信息系统安全水平基础上实现成本最小化.

1 相关文献综述

信息系统安全防护一般是指组织使用一种或

多种信息系统安全技术来缓解或消除信息系统所面临的主要威胁.这不仅是一个技术层面的问题,同时也是一个经济与管理层面的问题.近年来经济与管理层面的相关研究表现得更加热门,这个层面的研究已经开始从研究单一安全技术向多种安全技术转变.从近年来的文献中可以看出,这些单独的技术主要包括入侵检测技术^[5-8]、漏洞补丁管理技术^[3,9]等,由于研究的是单一安全技术,这些文献要么研究脆弱性水平本身,要么研究其他技术对信息系统安全的防护,而未涉及脆弱性水平对其他技术选择与配置的影响.专注于多种信息系统安全技术的文献通常研究的是信息系统安全技术的组合问题. Rubel等^[10]指出为了对信息系统进行纵深防御,防火墙和其他技术应当组合在一起构建一个多层防御网络.因为不同安全技术具有不同的威胁防御能力^[11],面对若干种可能面临的威胁,组织必须选择若干种合适的安全技术来对付它们. Tanaka等^[1]认为一个经济实体的信息系统安全投资决策取决于脆弱性水平,而 Gupta^[2]证明了信息系统的脆弱性为0几乎是不可能的. Gordon等^[12]建立了一个经济模型用以确定信息系统安全防护的最优化投资,该模型考虑了脆弱性以及当这些脆弱性被攻击所带来的潜

在损失. Bojanc 等^[13] 提出一个信息系统安全最优投资选择程序, 该程序不仅考虑了信息系统价值, 同时还考虑了其财产、威胁和脆弱性的识别问题. 不难发现, 这些关注系统脆弱性水平的研究大多局限于信息系统安全投资领域, 而极少涉及信息系统安全技术的选择与配置.

国内方面, 学者们对信息系统安全研究涉及的脆弱性水平多偏向于对信息系统安全风险或对脆弱性本身的评估, 如曹波等^[14] 构建了电力系统的脆弱性评估模型并通过算例验证了该模型的有效性; 吴金宇^[15] 提出脆弱性是网络攻击发生的必要条件之一; 戴迎春等^[16] 则对脆弱性本身的分类展开研究, 这些研究基本也没有将脆弱性水平同信息系统安全技术选择与配置联系在一起.

当组织选择了多种信息系统安全技术来对其信息系统进行防护时, 其需部署并配置这些技术, 使得这些技术之间相互配合、相互补充^[4]. 受文献^[4] 启发, 本文构建一个组织和黑客博弈模型, 重点研究脆弱性水平对组织信息系统安全技术策略的影响. 该模型不仅加入了信息系统脆弱性水平参数, 还将其与黑客入侵成功率进行量化联系. 模型最终还将给出组织所选择信息系统安全技术的最优配置, 以帮助其在信息系统安全防护中获得足够高(非最高)的安全水平和最低的安全成本.

2 模型构建

一个完整的博弈模型应当包括至少 3 类元素: 博弈参与者、参与者策略以及参与者策略的支付. 在本文将提出的模型中, 博弈双方为组织和黑客, 组织的策略为其各种信息系统安全策略, 而黑客的策略为攻击与不攻击两种.

2.1 模型描述

黑客入侵组织信息系统事件可被描述为如图 1 所示, 该图显示了信息系统被入侵事件的 3 个主要因素: 黑客、信息系统和黑客实施的攻击行为. 黑客入侵成功与否主要在于其是否找出信息系统脆弱性并对其加以利用, 从而导致组织发生损失, 而不管其入侵是否被组织监测到. 黑客能否找到脆弱性将受到组织信息系统脆弱性管理现状的影响, 即组织信息系统脆弱性水平将对黑客入侵成功率具有重要影响. 黑客入侵成功与否还受黑客能力及其努力程度影响, 但因这两个因素不在本文研究范围内, 假设发起入侵的黑客具有足够的能力和努力水平, 即忽略这两个因素对黑客

入侵成功率的影响.

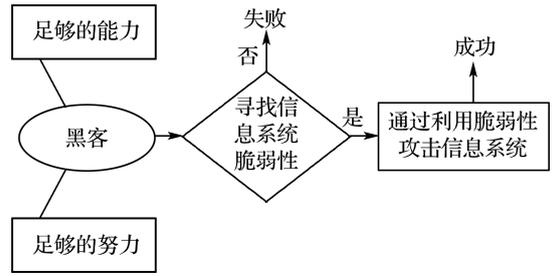


Fig. 1 Event of information system intruded by hackers

组织使用脆弱性扫描技术、补丁技术等较直接的方法降低系统脆弱性水平, 从而直接降低黑客入侵成功率. 假设其脆弱性水平为 P_s , 这里沿用了 Gordon 等^[12] 对脆弱性水平的定义, 即脆弱性是指威胁成功实现的概率, 并将组织维持某一系统脆弱性水平的成本记为 c_{t2} . 另外, 组织也选择了 IDS 对系统进行防护. IDS 具有两个重要的参数, 即 P_d^i 和 P_f^i ^[4], 其中 P_d^i 表示当入侵发生时, IDS 发出警报的概率, 而 P_f^i 则表示当入侵未发生时, IDS 发出警报的概率. IDS 发出的警报可用于警示信息系统管理人员发起调查从而进一步确定是否存在真实入侵, 并对真实入侵加以阻止和防范. 根据 IDS 发出的警报, 信息系统管理人员决定是否进行人工调查: 一般而言, 为减少浪费, 他们并不会对所有 IDS 警报事件进行调查, 因为 IDS 有时会在未发生入侵的情况下发出警报, 且人工调查费用也很高; 同时为了减少 IDS 漏报损失, 他们也会在 IDS 未发出警报的情况下进行一定程度的调查. IDS 发出警报情况下和未发出警报情况下的人工调查率不同, 分别用 ρ_1 和 ρ_2 表示, 同时用 c_{it} 来表示人工调查发生的费用. 当黑客成功入侵系统且未被组织检测出, 组织将遭受损失 d , 而其入侵成功但被检测出, 组织的损失记为 $(1 - \phi)d$, 其中假设组织发现入侵将采取一定措施以挽回一定比例损失, 记为 ϕ ($\phi \leq 1$). 另外由组织的经济理性, 即其只有在可挽回的损失大于其调查成本的情况下才会发起调查可知 $d\phi P_s > c_{it}$.

假设黑客选择入侵系统的概率为 ψ , 则其选择不入侵的概率为 $1 - \psi$. 黑客发起入侵的成本记为 c_h , 入侵成功的收益则记为 μ_h , 其入侵成功的概率为 P_s , 也就是组织信息系统脆弱性水平. 若入侵行为被组织人工检测到, 黑客将遭受到惩罚 β ,

则其净收益记为 $\mu_h P_s - c_h - \beta$, 其中 $\mu_h P_s - c_h - \beta < 0$, 这意味着不论入侵是否成功, 只要黑客入侵行为被组织检测到, 其收益将为负。

当组织同时使用漏洞扫描、补丁管理等技术致力于降低信息系统脆弱性的直接措施和使用 IDS 技术致力于降低黑客入侵率的间接措施时, 两种措施相互影响、相互制约, 如图 2 所示。

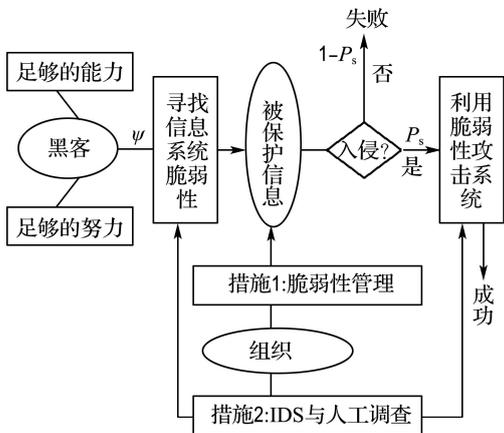


图 2 组织对信息系统安全防护的两种措施交互
Fig. 2 Interaction between two information system security countermeasures used by organization

图 2 在图 1 的基础上进一步展现了组织信息系统脆弱性水平和 IDS 技术之间的内在联系。脆弱性水平决定于措施 1, 而 IDS 检测率配置则取决于措施 2。两种措施同时采用时, 必然会对对方产生影响和限制, 这不仅是由组织信息系统安全成本投入有限决定的, 同时也是安全防护需求与防护原理的体现。

在本文的博弈模型中, 黑客的策略为攻击 (H) 与不攻击 (NH), 其策略集为 $S^h \in \{H, NH\}$, 组织的策略为在警报情形下调查 (I) 与不调查 (NI), 在未警报情形下调查 (I) 与不调查 (NI), 其策略集为 $S^i \in \{(I, I), (I, NI), (NI, I), (NI, NI)\}$, 其中每一对策略组合中, 前者表示警报情形下组织的选择, 后者表示未警报情形下组织的选择。这里假设组织和黑客均为风险中立者, 且两者之间是完全信息博弈。当组织组合使用脆弱性管理技术和 IDS 技术时, 其在警报情形下和未警报情形下的期望支付计算如下:

$$F_a(\rho_1, \psi) = -\rho_1 c_{fi} - P_{SHA}(1 - \rho_1)d - P_{SHA}\rho_1(1 - \phi)d - c_{f2}(1 - P_s)$$

$$F_{na}(\rho_2, \psi) = -\rho_2 c_{fi} - P_{SHNA}(1 - \rho_2)d - P_{SHNA}\rho_2(1 - \phi)d - c_{f2}(1 - P_s)$$

从而组织总期望支付记为

$$F(\rho_1, \rho_2, \psi) = P_a F_a(\rho_1, \psi) + P_{na} F_{na}(\rho_2, \psi)$$

黑客的期望收益如下:

$$H(\rho_1, \rho_2, \psi) = \mu_h \psi P_s - c_h \psi - \beta(\rho_1 P_d^i + \rho_2(1 - P_d^i))\psi$$

2.2 均衡的推导与分析

在上述模型中, 组织和黑客都欲最大化各自的收益。根据表 1 中给出的各概率表达式, 双方的均衡策略可通过计算推导出。

表 1 概率表达式汇总

Tab. 1 Summary of the expressions of probabilities

概率	表达式
P_a : IDS 发出警报的概率	$\psi P_d^i + (1 - \psi) P_i^i$
P_{na} : IDS 未发出警报的概率	$1 - \psi P_d^i - (1 - \psi) P_i^i$
P_{HA} : IDS 发出警报时黑客入侵的概率	$\frac{\psi P_d^i}{P_a}$
P_{SHA} : IDS 发出警报时黑客成功入侵的概率	$\frac{\psi P_d^i P_s}{P_a}$
P_{HNA} : IDS 未发出警报时黑客入侵的概率	$\frac{\psi(1 - P_d^i)}{1 - P_a}$
P_{SHNA} : IDS 未发出警报时黑客成功入侵的概率	$\frac{\psi(1 - P_d^i) P_s}{1 - P_a}$

定理 1 当组织实施脆弱性管理技术和 IDS 技术对其信息系统进行防护时, 博弈的均衡为

$$\rho_1^* = \frac{\mu_h P_s - c_h}{\beta P_d^i}, \rho_2^* = 0,$$

$$\psi^* = \frac{c_{fi} P_i^i}{P_d^i \phi d P_s - c_{fi}(P_d^i - P_i^i)};$$

$$\frac{c_h}{\mu_h} \leq P_s \leq \frac{P_d^i \beta + c_h}{\mu_h}$$

$$\rho_1^* = 1, \rho_2^* = \frac{\mu_h P_s - c_h - \beta P_d^i}{\beta(1 - P_d^i)},$$

$$\psi^* = \frac{c_{fi}(1 - P_i^i)}{(1 - P_d^i) \phi d P_s + c_{fi}(P_d^i - P_i^i)};$$

$$\frac{P_d^i \beta + c_h}{\mu_h} < P_s \leq 1$$

证明 组织在给定选择脆弱性管理技术和 IDS 技术组合条件下, 其在警报情形下和未警报情形下的期望支付计算如下:

$$F_a(\rho_1, \psi) = -\rho_1 c_{fi} - \frac{\psi P_d^i P_s}{\psi P_d^i + (1 - \psi) P_i^i} \times (1 - \rho_1)d - \frac{\psi P_d^i P_s}{\psi P_d^i + (1 - \psi) P_i^i} \times \rho_1(1 - \phi)d - c_{f2}(1 - P_s)$$

$$F_{na}(\rho_2, \psi) = -\rho_2 c_{fi} - \frac{\psi(1 - P_d^i) P_s}{1 - \psi P_d^i - (1 - \psi) P_i^i} \times$$

$$(1 - \rho_2)d - \frac{\psi(1 - P_d^i)P_s}{1 - \psi P_d^i - (1 - \psi)P_f^i} \times \\ \rho_2(1 - \phi)d - c_{f2}(1 - P_s)$$

黑客发起入侵的期望收益为

$$H(\rho_1, \rho_2, \psi) = \mu_h \psi P_s - c_h \psi - \beta(\rho_1 P_d^i + \\ \rho_2(1 - P_d^i))\psi$$

不论是在警报情形下还是在未警报情形下,组织都想最大化其收益,此时对 $F_a(\rho_1, \psi)$ 的变量 ρ_1 和 $F_{na}(\rho_2, \psi)$ 的变量 ρ_2 分别进行一阶求导如下:

$$\frac{\partial F_a(\rho_1, \psi)}{\partial \rho_1} = -c_{f1} + \frac{\psi P_d^i P_s d \phi}{\psi P_d^i + (1 - \psi)P_f^i} \quad (1)$$

$$\frac{\partial F_{na}(\rho_2, \psi)}{\partial \rho_2} = -c_{f1} + \frac{\psi(1 - P_d^i)P_s d \phi}{1 - \psi P_d^i - (1 - \psi)P_f^i} \quad (2)$$

黑客欲最大化其入侵收益,此时对其收益 $H(\rho_1, \rho_2, \psi)$ 的变量 ψ 求一阶导数如下:

$$\frac{\partial H(\rho_1, \rho_2, \psi)}{\partial \psi} = \mu_h P_s - c_h - \beta(\rho_1 P_d^i + \\ \rho_2(1 - P_d^i)) \quad (3)$$

当 $\frac{\partial H(\rho_1, \rho_2, \psi)}{\partial \psi} = 0$ 时,黑客将会得到其最大化收益,即:

$$\frac{\partial H(\rho_1, \rho_2, \psi)}{\partial \psi} = \mu_h P_s - c_h - \beta(\rho_1 P_d^i + \\ \rho_2(1 - P_d^i)) = 0$$

当 $\frac{\partial F_a(\rho_1, \psi)}{\partial \rho_1} = \frac{\partial F_{na}(\rho_2, \psi)}{\partial \rho_2} = 0$ 时,组织将会得到其最大化的支付,但对于同一黑客入侵率 ψ , $\frac{\partial F_a(\rho_1, \psi)}{\partial \rho_1}$ 和 $\frac{\partial F_{na}(\rho_2, \psi)}{\partial \rho_2}$ 无法同时为 0,且研究能

证明出 $\frac{\partial F_a(\rho_1, \psi)}{\partial \rho_1} \geq \frac{\partial F_{na}(\rho_2, \psi)}{\partial \rho_2}$:

$$\frac{\partial F_a(\rho_1, \psi)}{\partial \rho_1} - \frac{\partial F_{na}(\rho_2, \psi)}{\partial \rho_2} = \\ -c_{f1} + \psi P_d^i P_s d \phi / [\psi P_d^i + (1 - \psi)P_f^i] + \\ c_{f1} - \psi(1 - P_d^i)P_s d \phi / [1 - \psi P_d^i - (1 - \psi)P_f^i] = \\ [(1 - \psi P_d^i - (1 - \psi)P_f^i)P_d^i - (\psi P_d^i + (1 - \psi)P_f^i)] \times \\ (1 - P_d^i)] d \phi P_s \psi / [(\psi P_d^i + (1 - \psi)P_f^i) \times \\ (1 - \psi P_d^i - (1 - \psi)P_f^i)] = \\ [P_d^i - (\psi P_d^i + (1 - \psi)P_f^i)] d \phi P_s \psi / [(\psi P_d^i + \\ (1 - \psi)P_f^i)(1 - \psi P_d^i - (1 - \psi)P_f^i)] = \\ [(1 - \psi)P_d^i - (1 - \psi)P_f^i] d \phi P_s \psi / [(\psi P_d^i + \\ (1 - \psi)P_f^i)(1 - \psi P_d^i - (1 - \psi)P_f^i)] = \\ [(1 - \psi)(P_d^i - P_f^i)] d \phi P_s \psi / [(\psi P_d^i + \\ (1 - \psi)P_f^i)(1 - \psi P_d^i - (1 - \psi)P_f^i)] \quad (4)$$

在式(4)中,由于 $1 - \psi \geq 0$ (其中 $\psi \in [0, 1]$), $\psi P_d^i + (1 - \psi)P_f^i \geq 0, 1 - \psi P_d^i - (1 - \psi)P_f^i \geq 0,$

$d \phi P_s \psi \geq 0, P_d^i - P_f^i \geq 0$ (其中 $P_f^i = (P_d^i)^r, r \in [0, 1]$)[4]), 则 $\frac{\partial F_a(\rho_1, \psi)}{\partial \rho_1} \geq \frac{\partial F_{na}(\rho_2, \psi)}{\partial \rho_2}$, 根据此条件可

计算出次优均衡结果,即在 $\frac{\partial F_a(\rho_1, \psi)}{\partial \rho_1} = 0 > \frac{\partial F_{na}(\rho_2, \psi)}{\partial \rho_2}$ 或 $\frac{\partial F_a(\rho_1, \psi)}{\partial \rho_1} > \frac{\partial F_{na}(\rho_2, \psi)}{\partial \rho_2} = 0$ 这两种情形下的均衡。

情形 1 $\frac{\partial F_a(\rho_1, \psi)}{\partial \rho_1} = 0 > \frac{\partial F_{na}(\rho_2, \psi)}{\partial \rho_2}$ 且

$$\frac{\partial H(\rho_1, \rho_2, \psi)}{\partial \psi} = 0$$

$$\text{由 } \frac{\partial F_a(\rho_1, \psi)}{\partial \rho_1} = -c_{f1} + \frac{\psi P_d^i P_s d \phi}{\psi P_d^i + (1 - \psi)P_f^i} = 0,$$

得 $\psi^* = \frac{c_{f1} P_f^i}{P_d^i \phi d P_s - c_{f1}(P_d^i - P_f^i)}$;

$$\text{由 } \frac{\partial F_{na}(\rho_2, \psi)}{\partial \rho_2} = -c_{f1} + \frac{\psi(1 - P_d^i)P_s d \phi}{1 - \psi P_d^i - (1 - \psi)P_f^i}$$

$< 0, \rho_2 \in [0, 1]$, 知 $\max F_{na}(\rho_2, \psi)$ 将在 $\rho_2^* = 0$ 处获得。

$$\text{将 } \rho_2^* = 0 \text{ 代入 } \frac{\partial H(\rho_1, \rho_2, \psi)}{\partial \psi} = \mu_h P_s - c_h -$$

$$\beta(\rho_1 P_d^i + \rho_2(1 - P_d^i)) = 0, \text{ 可得 } \rho_1^* = \frac{\mu_h P_s - c_h}{\beta P_d^i}.$$

由 $\rho_1^* \in [0, 1]$ 且 $0 \leq P_s \leq 1$, 得 $0 \leq$

$$\frac{\mu_h P_s - c_h}{\beta P_d^i} \leq 1, \frac{c_h}{\mu_h} \leq P_s \leq \frac{P_d^i \beta + c_h}{\mu_h}.$$

总之,情形 1 均衡为

$$\rho_1^* = \frac{\mu_h P_s - c_h}{\beta P_d^i}, \rho_2^* = 0,$$

$$\psi^* = \frac{c_{f1} P_f^i}{P_d^i \phi d P_s - c_{f1}(P_d^i - P_f^i)};$$

$$\frac{c_h}{\mu_h} \leq P_s \leq \frac{P_d^i \beta + c_h}{\mu_h}$$

情形 2 $\frac{\partial F_a(\rho_1, \psi)}{\partial \rho_1} > \frac{\partial F_{na}(\rho_2, \psi)}{\partial \rho_2} = 0$ 且

$$\frac{\partial H(\rho_1, \rho_2, \psi)}{\partial \psi} = 0$$

$$\text{由 } \frac{\partial F_{na}(\rho_2, \psi)}{\partial \rho_2} = -c_{f1} + \frac{\psi(1 - P_d^i)P_s d \phi}{1 - \psi P_d^i - (1 - \psi)P_f^i}$$

$= 0$, 得 $\psi^* = \frac{c_{f1}(1 - P_f^i)}{(1 - P_d^i)\phi d P_s + c_{f1}(P_d^i - P_f^i)}$;

$$\text{由 } \frac{\partial F_a(\rho_1, \psi)}{\partial \rho_1} = -c_{f1} + \frac{\psi P_d^i P_s d \phi}{\psi P_d^i + (1 - \psi)P_f^i} > 0,$$

$\rho_1 \in [0, 1]$, 知 $\max F_a(\rho_1, \psi)$ 将在 $\rho_1^* = 1$ 处获得。

$$\text{将 } \rho_1^* = 1 \text{ 代入 } \frac{\partial H(\rho_1, \rho_2, \psi)}{\partial \psi} = \mu_h P_s - c_h -$$

$$\beta(\rho_1 P_d^i + \rho_2(1 - P_d^i)) = 0, \text{ 可得 } \rho_2^* =$$

$$\frac{\mu_h P_s - c_h - \beta P_d^i}{\beta(1 - P_d^i)}$$

由 $\rho_2^* \in (0, 1]$ 且 $0 \leq P_s \leq 1$, 得 $0 <$

$$\frac{\mu_h P_s - c_h - \beta P_d^i}{\beta(1 - P_d^i)} \leq 1, \text{ 即 } \frac{P_d^i \beta + c_h}{\mu_h} < P_s \leq 1.$$

总之, 情形 2 均衡为

$$\rho_1^* = 1, \rho_2^* = \frac{\mu_h P_s - c_h - \beta P_d^i}{\beta(1 - P_d^i)},$$

$$\psi^* = \frac{c_{fi}(1 - P_f^i)}{(1 - P_d^i)\phi d P_s + c_{fi}(P_d^i - P_f^i)};$$

$$\frac{P_d^i \beta + c_h}{\mu_h} < P_s \leq 1$$

证毕.

从定理 1 首先可以看出, 组织的信息系统脆弱性水平取值范围为 $[\frac{c_h}{\mu_h}, 1]$, 而不是 $[0, 1]$, 这说明零脆弱性的信息系统是不存在的. 其次当脆弱性水平处于不同区间内, 组织和黑客的均衡策略是不同的. 当 $\frac{c_h}{\mu_h} \leq P_s \leq \frac{P_d^i \beta + c_h}{\mu_h}$ 时, 组织只需要

对 IDS 发出的部分警报发起调查, 而非对所有警报发起调查, 人工调查率 $\rho_1^* = \frac{\mu_h P_s - c_h}{\beta P_d^i}$, 同时对未发出警报的访问事件均采用不调查的策略; 当 $\frac{P_d^i \beta + c_h}{\mu_h} < P_s \leq 1$ 时, 意味着脆弱性水平提高到新的区间, 组织将会对所有警报事件发起调查, 同时也会对部分未警报事件发起调查, 人工调查率

$$\rho_2^* = \frac{\mu_h P_s - c_h - \beta P_d^i}{\beta(1 - P_d^i)}.$$

3 讨论与分析

根据模型及其结果, 脆弱性水平对安全技术策略具有若干重要影响, 从而产生了以下两个推论:

推论 1 在组织选定 IDS 与脆弱性管理技术相组合的前提下, 当系统脆弱性水平满足条件 $\frac{c_h}{\mu_h} \leq P_s \leq \frac{P_d^i \beta + c_h}{\mu_h}$ 时, 组织应部署具有较高检测率的 IDS.

证明 由定理 1 可知当 $\frac{c_h}{\mu_h} \leq P_s \leq \frac{P_d^i \beta + c_h}{\mu_h}$ 时,

$$\psi^* = \frac{c_{fi} P_f^i}{P_d^i \phi d P_s - c_{fi}(P_d^i - P_f^i)} \quad (5)$$

对式(5)进行变化得:

$$\psi^* = \frac{1}{\frac{P_d^i}{P_f^i} \frac{(\phi d P_s - c_{fi})}{c_{fi}} + 1} \quad (6)$$

根据 ROC 曲线^[7], $P_f^i = (P_d^i)^r$, $r \in [0, 1]$, 将其代入式(6)得

$$\psi^* = \frac{1}{P_d^{i(1-r)} \frac{(\phi d P_s - c_{fi})}{c_{fi}} + 1} \quad (7)$$

从式(7)可直观地看出当脆弱性水平一定时, 黑客入侵率将随着 IDS 检测率的提高而降低, 因此组织应配置较高检测率的 IDS 以保持较低的黑客入侵率.

证毕.

为了进一步分析推论 1 对实践的指导作用, 研究对其进行了仿真, 如图 3 所示.

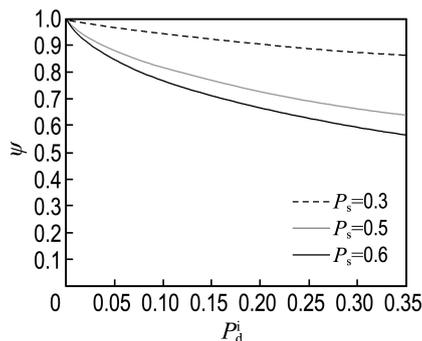


图 3 不同脆弱性水平下 IDS 检测率与黑客入侵率变化关系

Fig. 3 Relation between IDS detection rates and intrusion rates of hacker under different vulnerability levels

图 3 进一步假设各个常参数的值如下所示: $c_{fi} = 20, d = 150, \phi = 0.6, \mu_h = 100, \beta = 200, r = 0.25$, 其中 3 条曲线分别表示不同脆弱性水平条件下 IDS 入侵检测率与黑客入侵率之间的变化关系. 首先值得肯定的是在 $\frac{c_h}{\mu_h} \leq P_s \leq \frac{P_d^i \beta + c_h}{\mu_h}$ 条件下, 当脆弱性水平 P_s 一定时, 黑客入侵率将随着组织 IDS 检测率的提高而降低. 其次纵观 3 条曲线也不难发现随着脆弱性水平的提高, 同一 IDS 检测率下的黑客入侵率将有所降低. 表面上看, 这是一个悖论, 但是当组织运用脆弱性管理技术和 IDS 技术组合时可得到解释: 在 $\frac{c_h}{\mu_h} \leq P_s \leq \frac{P_d^i \beta + c_h}{\mu_h}$ 条件下, 组织信息系统脆弱性水平越高, 其部署的 IDS 检测率越高(黑客也这样认为, 且

其不知道具体检测率的值),此时黑客由于畏惧被IDS检测出而带来的较高惩罚不得不降低其选择入侵的可能性。

推论 2 当 $\frac{c_h}{\mu_h} \leq P_s \leq \frac{P_d^i \beta + c_h}{\mu_h}$ 时, $\rho_i^* = \frac{\mu_h P_s - c_h}{\beta P_d^i}$, 此时组织人工调查率与IDS入侵检测率呈反向变化关系,而与脆弱性水平呈正向变化关系。

推论 2 比较直观,从人工调查率的表达式 $\rho_i^* = \frac{\mu_h P_s - c_h}{\beta P_d^i}$ 可直接看出。这说明当脆弱性水平和IDS入侵检测率满足一定的关系时,均衡的人工调查率将随着IDS入侵检测率的提高而减小,同时将随着脆弱性水平的提高而提高。

4 结 语

随着信息系统环境的越来越复杂化,组织在信息系统防护过程中应选择多种安全技术以形成更为优化的安全技术策略。本文以IDS和人工调查技术组合为例,使用博弈论证明了脆弱性水平对组织信息系统安全技术运用与配置策略具有重要影响。首先,当脆弱性处于较低水平时,组织调查策略为对IDS警报事件进行部分调查,对未警报事件均不调查;而当脆弱性水平上升到新的区间时,组织的调查策略为对所有警报事件调查,对部分未警报事件调查。第二,在组织选定IDS技术与脆弱性管理技术相组合的前提下,当系统脆弱性水平满足条件 $\frac{c_h}{\mu_h} \leq P_s \leq \frac{P_d^i \beta + c_h}{\mu_h}$ 时,组织应部署具有较高检测率的IDS。该结论有趣之处在于黑客入侵率并不总是随着脆弱性水平(其入侵成功率)的增加而提高,尤其是当 $\frac{c_h}{\mu_h} \leq P_s \leq \frac{P_d^i \beta + c_h}{\mu_h}$ 时,两者之间俨然成反向变化趋势。这可用于指导那些追求信息系统脆弱性最小化时资金不足和技术能力一般的组织在防护其信息系统安全时,借助其他合适的信息系统安全技术及其配置对威胁的发生加以防范。第三,当 $\frac{c_h}{\mu_h} \leq P_s \leq \frac{P_d^i \beta + c_h}{\mu_h}$ 时, $\rho_i^* = \frac{\mu_h P_s - c_h}{\beta P_d^i}$, 此时组织人工调查率将随着脆弱性水平提高而提高。

上述结论显示出了一定程度的创新,如证明

了组织信息系统脆弱性水平对安全技术配置的影响,对组织人工调查率的影响等,但是本文依然存在一定的不足,需要进一步深入研究。第一,对于资金和技术能力均一般的组织,他们降低系统脆弱性的能力有限,除了选择像本文中提出的IDS技术、人工调查技术等来与脆弱性管理配合,其还可以选择其他安全技术,如防火墙技术、虚拟私网技术和蜜罐技术等。根据所选技术组合的不同,组织所需的最佳技术配置组合也是不同的。第二,当黑客的能力和水平并非本文中所假定的足够高时,这两个因素将在一定程度上影响黑客入侵成功率,从而改变黑客入侵成功率决定于组织脆弱性管理水平的定论,也将改变黑客入侵成功率与其选择入侵率之间的变化关系。第三,模型假设IDS警报与未警报情形下的人工调查率为独立变量,未来可通过模型重构进一步研究这两者之间的关系。

参 考 文 献:

- [1] Tanaka H, Matsuura K, Sudoh O. Vulnerability and information security investment: An empirical analysis of e-local government in Japan [J]. **Journal of Accounting and Public Policy**, 2005, 24(1): 37-59.
- [2] Gupta M. Matching information security vulnerabilities to organizational security profiles: A genetic algorithm approach [J]. **Decision Support Systems**, 2006, 41(3): 592-603.
- [3] Cavusoglu H, Cavusoglu H, Zhang J. Security patch management: Share the burden or share the damage? [J]. **Management Science**, 2008, 54(4): 657-670.
- [4] Cavusoglu H, Raghunathan S, Cavusoglu H. Configuration of and interaction between information security technologies: the case of firewalls and intrusion detection systems [J]. **Information Systems Research**, 2009, 20(2): 198-217.
- [5] XIA Zheng-you, ZHANG Shi-yong. A kind of network security behavior model based on game theory [C] // **Parallel and Distributed Computing, Applications and Technologies, PDCAT 2003 Proceedings**. Los Alamitos: IEEE Computer Society, 2003: 950-954.
- [6] Cavusoglu C, Mishra B, Raghunathan S. The value of intrusion detection systems in information technology security architecture [J]. **Information**

- Systems Research**, 2005, **16**(1):28-46.
- [7] Yue W T, Cakanyildirim M. Intrusion prevention in information systems: Reactive and proactive responses [J]. **Journal of Management Information Systems**, 2007, **24**(1):329-353.
- [8] Ogut H, Cavusoglu H, Raghunathan S. Intrusion-detection policies for IT security breaches [J]. **INFORMS Journal on Computing**, 2008, **20**(1):112-123.
- [9] August T, Tunca T I. Network software security and user incentives [J]. **Management Science**, 2006, **52**(11):1703-1720.
- [10] Rubel P, Ihde M, Harp S, *et al.* Generating policies for defense in depth [C] // **Proceedings - 21st Annual Computer Security Applications Conference, ACSAC 2005**. Los Alamitos: IEEE Computer Society, 2005:505-514.
- [11] Kumar R L, Park S, Subramaniam C. Understanding the value of countermeasure portfolios in information systems security [J]. **Journal of Management Information Systems**, 2008, **25**(2):241-279.
- [12] Gordon L A, Loeb M P. The economics of information security investment [J]. **ACM Transactions on Information and System Security**, 2002, **5**(4):438-457.
- [13] Bojanc R, Jerman-Blazic B. Towards a standard approach for quantifying an ICT security investment [J]. **Computer Standards and Interfaces**, 2008, **30**(4):216-222.
- [14] 曹波, 吴峥, 杨杉, 等. 电力监控系统脆弱性评估模型研究 [J]. **计算机与数字工程**, 2014, **42**(1):107-111.
CAO Bo, WU Zheng, YANG Shan, *et al.* Grid baseline security evaluation [J]. **Computer & Digital Engineering**, 2014, **42**(1):107-111. (in Chinese)
- [15] 吴金字. 网络安全风险评估关键技术研究 [D]. 北京: 北京邮电大学, 2013.
WU Jin-yu. Research on key technologies of network security risk assessment [D]. Beijing: Beijing University of Posts and Telecommunications, 2013. (in Chinese)
- [16] 戴迎春, 赵忠文. 基于信息安全属性的脆弱性分类方法 [J]. **计算机工程与应用**, 2012, **48**(S2):335-338.
DAI Ying-chun, ZHAO Zhong-wen. Vulnerability classification based on information security attributes [J]. **Computer Engineering and Applications**, 2012, **48**(S2):335-338. (in Chinese)

Study of influence of vulnerability level on information system security technology strategy

FANG Ling*, ZHONG Wei-jun, MEI Shu-e

(School of Economics and Management, Southeast University, Nanjing 211100, China)

Abstract: Game theory was used to learn organizations' information system security technology strategies based on the vulnerability level. It is found that the vulnerability level of an information system has important influence on the selection and configuration of an organization's information system security technologies. When the vulnerability level is comparatively low, the organization should only investigate some IDS alarms manually and ignore no-alarms. When the vulnerability level is comparatively high, the organization should investigate all IDS alarms and some no-alarms manually. Meanwhile, the manual investigation probability would increase with the improvement of the vulnerability level. Apart from these facts, when the vulnerability level of an information system is comparatively high, the probability of hacker intrusion is not always high because the organization has deployed an IDS with comparatively high intrusion detection rate.

Key words: vulnerability level; intrusion detection system configuration; manual investigation; information system security; hacker's success probability