DISTRIBUTED VULNERABILITY ASSESSMENT APPLIED TO MEASURING CITIZEN CYBER-HEALTH AND SECURING ONLINE PUBLIC SERVICES

Kálmán Hadarics[1], Ferenc Leitold[2] and Anthony Arrott[3]

Abstract
Since the introduction of personal computing over the Internet, cyber-security has developed primarily as commercial services providing protection to organizations and individuals as customers of paid services. However, since the introduction of cloud-services and smartphones over a decade ago, this development has been radically altered. Effective cyber-security can no longer be provided as simplistic protective walls around trusted zones of computing (for organizations: isolated private corporate networks with secure network gateways; for individuals: stand-alone personal computers protected by locally-running anti-virus applications). These approaches have always assumed that cyber-threats do not originate from inside trusted zones. Increasingly, cyber-security is more effectively achieved through detecting and mitigating vulnerabilities discovered through coordinated assessment of malware threats, user behaviors, and IT infrastructure weaknesses. Unlike the traditional focus on malware threats alone, this integrated approach treats the IT infrastructure and user behavior of each individual and each organization department separately. This distributed approach makes no assumptions about the origins of cyber-threats.

In this paper, we examine the implications of using this distributed approach in the public sector. Particular emphasis is placed on aspects where the traditional framework of cyber-security as a commercial service can be usefully abandoned and replaced by more effective public sector practices. The recent evolution of the Digital Divide in Central and Eastern Europe has not been a simple story of those with less opportunity and access (old, poor, less educated) being able close the gap by "catching up" with those of greater opportunity and access (young, wealthy, well educated). Rather, the closing of the Digital Divide has been achieved more through the adoption of very different digital activities provided through very differently organized services – activities and services that require very different public sector approaches to cyber-security. These include new approaches to measuring citizen cyber-health; making citizens savvier about their personal cyber-security; and providing more secure online public services.

Key words: *distributed vulnerability analysis, citizen cyber-health, public services cybersecurity.*

1. Introduction

Information technology remodels the way how businesses and public services operate. It makes tremendous opportunities to increase revenues, cut costs and provides new feasibilities for customers. However an enterprise needs to control and manage the security of digital information in order to retain value from IT. The most important problems are data breaching and the growth of cyber-attacks. These incidents can result in substantial financial losses for business, governments

[1] University of Dunaújváros, H-2400 Dunaújváros, Táncsics M. u. 1/A., hadarics@uniduna.hu
[2] Secudit Ltd., H-8200 Veszprém, Kupa utca 16., fleitold@secudit.com
[3] Secudit Ltd., H-8200 Veszprém, Kupa utca 16., aarrott@secudit.com

and individuals. In order to achieve digital enterprise success, effective security initiatives and targeted protections are necessary to reduce or mitigate security risks.

Information security becomes more and more wide-reaching and crucial for every enterprise network. Traditional firewalls and intrusion prevention systems unable to provide entirely sufficient protection from malicious activities. Operational technology and the Internet of Things (IoT) [13] massively expand the scope of security strategy and operations. All systems, networks and application require a through and continuous review of all aspects of security. It includes everything from policy and planning to technologies, deployment, operations, and upgrades. In order to be able to maintain foundational IT capabilities and services security awareness trainings, employee behavior monitoring also necessary.

Network and system administrators are faced with different types of network attacks, and try to mitigate their impact. These attacks may come with different forms of malware, like viruses, worms, botnets or other types of intrusion. Even though the effectiveness of security controls to protect information is increasing, people may remain susceptible to manipulation.

Cybersecurity metrics generally combine results of protected IT (e.g., ongoing penetration testing) [14], malicious activities (e.g., breach detection testing) [15] and user behavior monitoring (e.g. probing user responses with fake phishing) [16, 17, 18]

Three distinct but highly interactive sources of vulnerability are considered [1]:

(1) Malicious activity by those who would subvert network capabilities for their own gain in violation of intended trusted relationships within the protected IT network;

(2) Disruptive and dangerous IT behaviors by network users (e.g., employees, customers, suppliers) in using IT network capabilities; and

(3) Unprotected vulnerabilities in the IT network infrastructure.

2. The triunal model of cyber-health

We adopt the concept of citizen cybersecurity [2]. Citizen cybersecurity becomes relevant to government agencies when citizens use their own personal computers to transact business with government, as in passport applications or online voting [3]. Both citizen trust and government technical efficacy rely on the integrity of online computer interactions between citizen and government [4]. Any real or perceived vulnerability of citizen-government information transactions to malicious activity undermines this integrity. The collective condition of each citizen's cybersecurity is thus a relevant matter for government. We call this collective condition citizen cyber-health [5]. Citizen cyber-health becomes relevant when a citizen's personal computer becomes infected with malware. A malware-infected personal computer may act against the interest of both the citizen and the government.

Consider an analogy with online banking: a depositor's malware-infected personal computer may act against the interest of both the depositor and the bank – no matter the security of the bank's servers and applications. Just as banks have an interest in the cyber-health of their online customers' computers, so governments have an interest in the cyber-health of their citizens' personal computers when they are used for online government activities.

Despite the best efforts of IT service providers, government regulators and law enforcement, responsibility for online security falls chiefly on individual citizens, whether as family members, employees, or government officials [6]. Measures of individual citizen cybersecurity health are useful indicators of broader citizen cyber-health vulnerabilities – especially for monitoring system activity, identifying and predicting areas for improvement, and evaluating ongoing changes [7, 8].

Vulnerability assessment may be thought of as the outermost layer in the ongoing provision of enterprise cybersecurity. The succeeding layers include: vulnerability detection, vulnerability remediation, security incident preparedness, security incident detection, and security incident response (Figure 1).

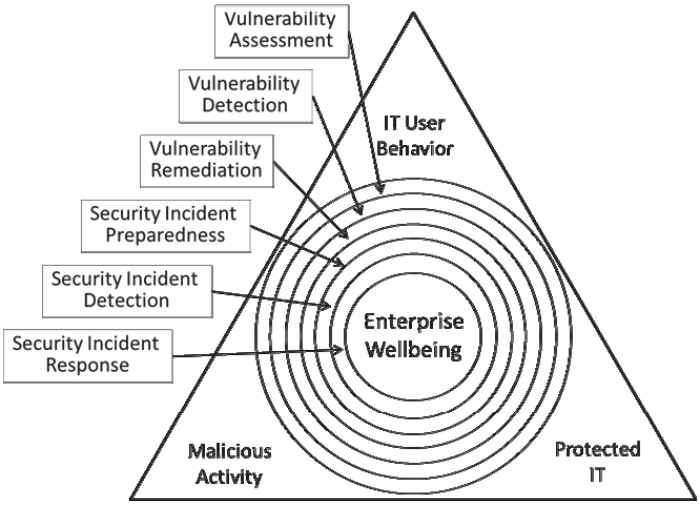

Figure 1: Vulnerability assessment within the context of overall cybersecurity contribution to enterprise wellbeing

To effectively contribute to enterprise wellbeing, vulnerability management requires practical and useful correlation of the various and highly interactive sources of vulnerability. The analogous requirement for security incident response is typically satisfied by security event information management systems (SEIM) [9]. For vulnerability management, we have adopted what we define as the Triunal Model of Cybersecurity Vulnerability. Derived from earlier formulations [10, 11], the triunal model decomposes vulnerability assessment into three contributing sources, or triunes: i) malicious activity; ii) unprotected IT; and iii) facilitating adverse user behavior. Within each contributing source, specific contributing factors are identified and characterized (e.g., social engineering and exploits within the malicious activity triune). The model provides a basis for correlating and combining contributing factors into an integrated view of specific vulnerabilities [12].

3. Estimating the vulnerability level

In an earlier publication [1] the basic components and assumptions of our vulnerability assessment method are defined. There are numerous threats that can have impact on the vulnerability level of an examined infrastructure. The vulnerability level of the infrastructure is defined as a probability of at least one threat is able to be executed on at least one device used by the given users in the infrastructure.

In order to be able to create a formal description et us define the followings:

L: set of all available threat landscapes (e.g.: World, Europe, USA, Hungary, …)
T_{all}: set of all possible malware
(note: at this moment we are focusing of the subset of threats, we are dealing with only the programmed attacks)
T_l: set of all possible malware inside $l \in L$, $T_l \subset T_{all}$

U: set of all users
I: set of all possible devices
P: set of all available protections
UT: set of all possible user tricks used by any malware in T

An integrated measure of vulnerability can be derived accounting for all three sources (attacker ingenuity, infrastructure weakness, adverse user behavior). For any given malware or class of malware for which the requisite IT infrastructure vulnerability and user facilitation is known, we can obtain a best estimate of:

1. The probability that an attacker will use a particular malware or class of malware against the enterprise (p_{prev}):

$$p_{prev}(t,l) = \frac{number\ of\ computers\ infected\ by\ \boldsymbol{t}\ inside\ \boldsymbol{l}}{number\ of\ all\ computers\ inside\ \boldsymbol{l}}$$

where $t \in T_l$ and $l \in L$;

2. The probabilities that the enterprise's IT infrastructure will allow the attack to be carried out successfully (p_{device}):

$$p_{prot}(t,p) = \frac{number\ of\ successfull\ attempts\ of\ \boldsymbol{t}\ thru\ the\ protection\ \boldsymbol{p}}{number\ of\ all\ attempts\ of\ \boldsymbol{t}\ thru\ the\ protection\ \boldsymbol{p}}$$

where $t \in T_l$, $l \in L$ and $p \in P$;

$$p_{device-prot}(t,i) = \min_{for\ all\ p\ protecting\ i} p_{prot}(t,p)$$

where $t \in T_l$, $l \in L$ and $i \in I$;

$$p_{device-elements}(t,i) = \begin{cases} 1, & if\ t\ can\ work\ on\ i \\ 0, & if\ t\ can\ not\ work\ on\ i \end{cases}$$

where $t \in T_l$, $l \in L$ and $i \in I$;

$$p_{device}(t,i) = p_{device-elements}(t,i) \cdot p_{device-prot}(t,i)$$

where $t \in T_l$, $l \in L$ and $i \in I$;

3. The probability that users of the enterprise's IT infrastructure will provide sufficient facilitation for the attack to succeed ($p_{usertrick}$, p_{user}, p_{usage}):

$$p_{usertrick}(t,ut) = \frac{number\ of\ attempts\ of\ \boldsymbol{t}\ where\ t\ used\ \boldsymbol{ut}}{number\ of\ all\ attempts\ of\ \boldsymbol{t}}$$

where $\in T_l$, $l \in L$, $ut \in UT$;

$$p_{user}(u, ut) = \frac{number\ of\ successfull\ attempts\ of\ \boldsymbol{ut}\ on\ \boldsymbol{u}}{number\ of\ all\ attempts\ of\ \boldsymbol{ut}\ on\ \boldsymbol{u}}$$

where $u \in U$, $ut \in UT$;

$$p_{usage}(u, i) = \frac{all\ time\ when\ u\ used\ i}{measuring\ interval}$$

where $u \in U$, $i \in I$;

The three main input classes (p_{prev}, p_{device}, $p_{usertrick}$ and p_{user}) can be combined to obtain an overall probability of malicious success (provided each relevant combination of attack, user, and component of IT infrastructure is accounted for):

$$q(l, i, ut) = 1 - \prod_{t}(1 - p_{usertrick}(t, ut) \cdot p_{prev}(t, l) \cdot p_{device}(t, i))$$

where $u \in U$, $i \in I$, $t \in T_l$, $l \in L$;

$$r(l, u, i) = 1 - \prod_{ut}(1 - q(l, i, ut) \cdot p_{user}(u, ut))$$

where $u \in U$, $i \in I, ut \in UT$, $l \in L$;

$$s(l) = 1 - \prod_{u,i}(1 - r(l, u, i) \cdot p_{usage}(u, i))$$

where $u \in U$, $i \in I$ and $l \in L$;

Separately measured combined probabilities of malicious success (p_{s1}, p_{s2}, p_{s3}, …) can be compared and prioritized. Subsequently, an identified high priority vulnerability (p_{si}) can be decomposed into its constituent vulnerability sources (p_{ai}, p_{bi}, p_{ci}) allowing remedial actions to be directed where the greatest measureable improvement can be made.

The calculated *s(l)* is a metric related to the vulnerability level of an organization using the calculated devices by the calculated users against the calculated threats. As it is a probability it has to be in the [0,1] interval and the higher value means more vulnerable situation. If the elements (threats, devices and users) are fixed then by adding any new element the *s(l)* vulnerability level will be the same or it will be increased.

4. The effect of correlation

The earlier introduced formulas are proper only if the introduced probabilities are independent from each other. In real life this ideal situation rarely occurs.

On the one hand we identify correlation between two elements of the triunial model. For example *threat1* can open a backdoor on a targeted system, and *threat2* can use that opened communication channel for its distribution. This exactly means that above formula needs to be extended towards conditional probabilities.

On the other hand if the state of a system are known, the probability of the another similar system are in the same state are greater if exist some type of relationship between them. For example let us

consider there are two cities *city A* and *city B*. Denote *p(A)* the probability of the weather in *city A* is rainy, *p(B)* should be the same for *city B*. If the cities are not so far from each other the difference between *p(A)* and *p(B)* can't be any size.

If we want to estimate that one of the cities the weather is rainy the probability of that (p_r)

$p_r <= 1-(1-p(A))*(1-p(B))$

In this case we can estimate with another formula p_r probability:

$p_r >= max(p(A), p(B))$

Writing these formulas together:

$max(p(A), p(B)) <= p_r <= 1-(1-p(A))*(1-p(B))$

This exactly means that the p_r probability are limited and exact value of that depends on correlation of different factors.

In this example it can be determined that distance mainly influences the likelihood of the same event. It also can be considered that the root cause of the state can be the same. The level of correlation will determine that the lower bound or upper bound estimate will produce better estimate.

If we want to adopt this into estimating the cyber-health of an information system we need to identify common factors someway and our estimate formula can be more accurate.

5. Conclusion

In this paper we demonstrate that the triunal model of cybersecurity vulnerability is largely fit to model cyber health. All important aspect of cybersecurity vulnerability are considered. The probabilities used in formulas can be calculated evaluating properties of threats, IT infrastructure component, user behavior and applied protections. In order to improve the estimation we need to consider correlation between components of our model.

6. References

[1] LEITOLD, F., ARROTT, A. and HADARICS, K.: Quantifying cyber-threat vulnerability by combining threat intelligence, IT infrastructure weakness, and user susceptibility 24th Annual EICAR Conference, Nuremberg, Germany, 2016.

[2] HARKNETT, R. J. and STEVER, J. A.: The cybersecurity triad: Government, private sector partners, and the engaged cybersecurity citizen. Journal of Homeland Security and Emergency Management 6.1, 2009.

[3] HILBERT, M.: The maturing concept of e-democracy: from e-voting and online consultations to democratic value out of jumbled online chatter. Journal of Information Technology and Politics, 6.2, 2009, p. 87–110.

[4] JORBA, A. R., RUIZ, J. A. O. and BROWN, P.: Advanced security to enable trustworthy electronic voting. Third European Conference on e-Government, 2003.

[5] ARROTT, A., LALONDE LEVESQUE, F., BATCHELDER, D. and FERNANDEZ, J. M.: Citizen cyber-security health metrics for Windows computers. Proceedings of Central and Eastern European eGov Days Conference, CEEEGOV, Budapest, Hungary, 2016.

[6] AHN, M. J., PARK, T.H. and LIM, C.H.: What Matters in Cybersecurity? The Role of Citizen Perception and Attributes. IJeN 3.1, 2015, p. 1-22.

[7] BERTOLLO, P.: Assessing ecosystem health in governed landscapes: a framework for developing core indicators. Ecosystem health, 4(1), 1998, p. 33–51.

[8] KSHETRI, N.: Cybercrime and Cybersecurity in the Middle East and North African Economies. Cybercrime and Cybersecurity in the Global South. Palgrave Macmillan UK, 2013.

[9] Microsoft. Evolution of malware and the threat landscape – a 10-year review, 2012.

[10] LEITOLD, F. and HADARICS, K.: Measuring security risk in the cloud-enabled enterprise. Malicious and Unwanted Software (MALWARE), 7th International Conference on Malicious and Unwanted Software, 2012, pp: 62-66.

[11] LEITOLD, F.: Security Risk analysis using Markov Chain Model. 19th Annual EICAR Conference, Paris, France, 2010.

[12] LEITOLD, F., ARROTT, A. and HADARICS, K.: Automating visibility into user behavior vulnerabilities to malware attack, Proceedings of the 26th Virus Bulletin International Conference (VB2016), pp. 16-24, Denver, USA, 2016.

[13] URIBEETXEBERRIA, R., ESKOLA, M.G., TRONO, L., GALILEO, S., MOVATION, J.N., DE CELIS ACORDE, L., MORGANI, A., SELEX, E.S., BALDELLI, R., TECNALIA, I.E. and HAI, N.P.: New embedded systems architecture for multi-layer dependable solutions. http://www.newshield.eu/wp-content/uploads/2013/11/ NSHIELD-D8.6_Build_Secure _Systems_with_SHIELD_v2.pdf

[14] Pwnie Express, Vulnerability assessment and penetration testing across the enterprise, Whitepaper, 2014, http://www.pwnieexpress.com

[15] EDWARDS, S.E., FORD, R. and Szappanos, G.: Effectively testing APT defenses. Virus Bulletin Conference, Prague, Czech Republic, 2015.

[16] CHAPMAN, M.T.: Advanced Persistent Testing: How to fight bad phishing with good, PhishLine, 2015, http://www.phishline.com/advanced-persistent-testing-ebook

[17] CHAPMAN, M.T.: Establishing metrics to manage the human layer. ISSA Security Education Awareness Special Interest Group, 2013.

[18] LALONDE LEVESQUE, F., FERNANDEZ, J. M., and SOMAYAJI, A.: Risk prediction of malware victimization based on user behavior. Malicious and Unwanted Software: The Americas (MALWARE), 2014 9th International Conference on IEEE, 2014.