DOGANA: Research on Human element advanced vulnerability assessment

Bernardo Pacheco, Nelson Escravana
Cybersecurity Unit
INOV INESC Inovação
Lisbon, Portugal
{bernardo.pacheco, nelson.escravana}@inov.pt

***Abstract*— Social Engineering vulnerability assessment poses challenges on the technical, psychological, ethical, moral and legal domains. This paper presents the key aspects of DOGANA project which addresses those domains aiming to develop a framework that encompasses state of the art technological tools for preforming SDVAs, while respecting ethical and legal boundaries. The approach will be validated with different mitigation strategies, that can be used by organizations to reduce their risk after performing these assessments.**

Keywords— Social Engineering; Vulnerability Assessment

I. INTRODUCTION

Cybersecurity implies the security of a complex system which includes the security of traditional information and communication systems, the organizations where those systems operate (physical conditions, processes, procedures, etc.) and the way that those systems are operated, that is: the human element. Social Engineering (SE), in the context of cybersecurity, has become integral to attack strategies [1] and is present in the large majority of cybersecurity incidents [2].

With the proliferation of usage of mobile computation devices and the amount of information that people make available online (e.g. social media), or is somehow accessible (e.g. cloud systems) the vulnerable attack surface keeps growing at an alarming rate. Additionally, attacks can be performed without requiring that much specialized skills.

Either during design, implementation or management of information systems, risk management and vulnerability assessment have traditionally been fundamental tools to understand and prioritize the effort (and investment) on securing a given system [3]. When referring to computer software, hardware or communication protocols, penetration testing has been a powerfully tool to identify vulnerabilities on systems [4]. But if SE is such an important aspect of the kill chain [5], not understanding how vulnerable an organization is to SE attacks is overlooking a key aspect of security. To assess vulnerabilities of the human factor, one could perform a Social Driven Vulnerability Assessment (SDVA).

To better understand the challenges of a SDVA for an organization, one needs to bear in mind that, unlike IT systems, employees are not owned by organizations, they have rights, namely to privacy. Therefore, SDVAs present challenges on technical, psychological, ethical, moral and legal domains.

DOGANA project [6] addresses those domains and aims to develop a framework that delivers "aDvanced sOcial enGineering And vulNerability Assessment" putting together state of the art technological tools for preforming SDVAs, while ensuring full compliance with European legislation and taking into consideration the psychological, ethical and privacy aspects of such an activity. The project also aims on building and testing different awareness methods, that can be suggested to organizations based on the results of a SDVA.

II. PRESENTING THE DOGANA APPROACH

DOGANA starts by exploring the SE attack anatomy, agreeing on a division of a SE attack into 4 different stages: information gathering, development of relationship, exploitation of relationship and execution of the attack to achieve an objective (this last stage is often a more technical one). To support this analysis, a Victim Communication Stack (VCS) is proposed [7] which in a similar way to the ISO/OSI stack, divides the communication with a victim into a set of layers to facilitate choosing the proper human attack vector.

A. SDVA model

From the high-level gap analysis of possible tools [8], the DOGANA framework approach to perform a SDVA to an organization is defined into the following four-step model:

- Information Gathering and Analysis Services (IGAS): At this stage, information about the targets are collected and turned into actionable intelligence. In addition to the information supplied by the organization, information is gathered from publically available online sources. E.g.: public profiles in social networks or contributions to blogs and web pages. Sensitive information is filtered out or discarded;
- Attack and Hook Preparation (AHP): After collecting information, in the second step the tester defines the approach to bait the targets and prepares the necessary resources to do it (e.g.: emails, SMS templates, web sites, etc.);
- Execution of the Attacks (EOA): At this stage. the simulated attacks are triggered by sending messages to the selected participants in the assessment. These messages are written in a way to convince targets to take specific actions (e.g.: open attachments, visit web

sites, fill-in personal information, etc.). Vulnerabilities are assessed by tracking their individual reactions;

- Information Aggregation and Reporting (IAR): At last, analysis of attack results is performed and reported. Clustering results makes it possible to link assets and vulnerabilities avoiding identification of participants.

B. Victim Communication Stack

Decisions taken during the AHP phase influence the way that the SDVA baits the targets. Starting from the information collected at IGAS phase, hook preparation must take in consideration these 6 levels of the VCS:

- Persona modelling, using available information about the target and taking into consideration dimensions such as personality, biographical data, social role/network, cultural background, etc.;
- Semantic, deals with persuasion techniques considered according to the "persona modelling";
- Syntax, includes elements selected as content of the message, for example wording, tone, graphics, etc.;
- Medium, addresses the selection of how the message is delivered (e.g.: SMS, email, phone call, etc.);
- Device, deals with the actual device where the message will be delivered to the user (e.g. phone, PC, etc.);
- Context, addresses all the environment surrounding the actual execution of the attack (e.g. time and place).

The VCS data is used for the EOA phase, making it possible for each attack to identify what were the decisions taken filling each layer and why they were considered effective, or not, in their goals.

C. Privacy by design

The privacy by design principles were adopted since the beginning of the DOGANA framework conceptual discussions and were kept during all development steps [9]. The goal of the resulting tool is to accurately assess the organizations' vulnerability, clustering without identifying the SDVA participants. Main adopted principles are:

- Consent of participants is mandatory and system allows the exclusion and removal of related information;
- Information must be related to the participants and stored only during the assessment;
- Tools requires authorized testers' authentication and actions will be recorded;
- Data collection will be limited to publicly available sources, and only the professional contacts will be used (any personal contact collected will be discarded). Any information that allows identification will be anonymized during the collection phase;
- Professional contacts should be kept in the system but at the operating interfaces it will be replaced by a unique and persistent but anonymous code;
- During credentials harvesting simulation, they will not be collected. Only evidences of actions will be stored;
- Any sensitive information will be discarded at the collection stage, including racial or ethnic origin, political philosophical opinions, religious beliefs, union or partisan registration, genetic data processing, biometric or health status, as well as sexual orientation.

III. Validation

The DOGANA framework will be validated through the execution of four different field trials. Each end-user, organization will independently run an internal SDVA and evaluate the framework effectiveness. These tests will cover a wide range of business sectors including transport, safety, military and governmental organizations from four different countries: Romania, Denmark, Greece and Portugal.

IV. Conclusions

The DOGANA project is researching a sound approach to perform SDVA, the results will be validated in relevant environments and the resulting tools are expected to improve the way that organizations deal with the assessment and mitigation of SE vulnerabilities. The framework is also being designed in way to significantly reduce the amount of effort (and cost) of performing a SDVA, making them more achievable by common / smaller organizations.

Acknowledgment

This work has been partially supported by the DOGANA project. DOGANA is a project funded by the European Union Horizon 2020 framework programme, under grant agreement number 653618.

References

[1] D. Ariu, E. Frumento, and G. Fumera, 'Social Engineering 2.0: A Foundational Work: Invited Paper', 2017, pp. 319–325.

[2] 'Verizon 2017 Data Breach Investigations Report', Verizon, 2017.

[3] R. Baskerville, 'Information systems security design methods: implications for information systems development', ACM Comput. Surv. CSUR, vol. 25, no. 4, pp. 375–414, 1993.

[4] B. Arkin, S. Stender, and G. McGraw, 'Software penetration testing', IEEE Secur. Priv., vol. 3, no. 1, pp. 84–87, 2005.

[5] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, 'Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains', Lead. Issues Inf. Warf. Secur. Res., vol. 1, no. 1, p. 80, 2011.

[6] 'DOGANA project'. [Online]. Available: https://www.dogana-project.eu/. [Accessed: 14-Sep-2017].

[7] E. Frumento, F. Freschi, D. Andreoletti, and A. Consoli, 'Victim Communication Stack (VCS): A flexible model to select the Human Attack Vector', in Proceedings of the 12th International Conference on Availability, Reliability and Security ACM, 2017, pp. 1–6.

[8] C. Dambra, A. G. PRO, E. Frumento, R. Puricelli, and F. Valentini, 'D3. 1 Report on existing tools, their evaluation and the gap to be filled by DOGANA development', DOGANA project, Jul. 2016.

[9] Filipe Custódio et al., 'D5.2 Legal Requirements for Privacy by Design', DOGANA project, Jun. 2015.