Digital Investigation 22 (2017) 62–73

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

Enhancing security incident response follow-up efforts with lightweight agile retrospectives

George Grispos [a, *], William Bradley Glisson [b], Tim Storer [c]

[a] School of Interdisciplinary Informatics, University of Nebraska at Omaha, Omaha, NE, United States
[b] School of Computing Science, University of South Alabama, Mobile, AL, United States
[c] School of Computing Science, University of Glasgow, Glasgow, Scotland, United Kingdom

ARTICLE INFO

Article history:
Received 23 November 2016
Received in revised form
7 June 2017
Accepted 27 July 2017
Available online 26 August 2017

Keywords:
Security incident response
Security investigations
Case study
Retrospectives
Incident learning

ABSTRACT

Security incidents detected by organizations are escalating in both scale and complexity. As a result, security incident response has become a critical mechanism for organizations in an effort to minimize the damage from security incidents. The final phase within many security incident response approaches is the feedback/follow-up phase. It is within this phase that an organization is expected to use information collected during an investigation in order to learn from an incident, improve its security incident response process and positively impact the wider security environment. However, recent research and security incident reports argue that organizations find it difficult to learn from incidents.

A contributing factor to this learning deficiency is that industry focused security incident response approaches, typically, provide very little practical information about tools or techniques that can be used to extract lessons learned from an investigation. As a result, organizations focus on improving technical security controls and not examining or reassessing the effectiveness or efficiency of internal policies and procedures. An additional hindrance, to encouraging improvement assessments, is the absence of tools and/or techniques that organizations can implement to evaluate the impact of implemented enhancements in the wider organization. Hence, this research investigates the integration of lightweight agile retrospectives and meta-retrospectives, in a security incident response process, to enhance feedback and/or follow-up efforts. The research contribution of this paper is twofold. First, it presents an approach based on lightweight retrospectives as a means of enhancing security incident response follow-up efforts. Second, it presents an empirical evaluation of this lightweight approach in a Fortune 500 Financial organization's security incident response team.

Introduction

Information security incidents continue to escalate in today's highly integrated business environments. According to a recent survey, a quarter of all businesses in the United Kingdom detected a security incident in the previous twelve months (Klahr et al., 2016). The consequences of such incidents for an organization can include significant financial losses, a loss of customer confidence and a reduction in business reputation (Ponemon Institute, 2015). In an effort to address information security incidents, many organizations have chosen to create security incident response teams (Killcrece et al., 2003; Mitropoulos et al., 2006). The objective of a security incident response team is to minimize the damage from a security incident, and to allow an organization to ultimately learn about the cause of the incident and how it can be prevented in the future (Mitropoulos et al., 2006).

In the past decade, several security incident response processes and best practice guidelines have been published in industry (Grance et al., 2004; International Organization for Standardization and International Electrotechnical Commission, 2011; Northcutt, 2001) and academia (Mitropoulos et al., 2006; Prosise et al., 2003; Vangelos, 2011), defining how organizations can investigate and manage a security incident. Typically, these incident response approaches consist of six phases: *preparation*, which leads to the *detection* of an incident, followed by its *containment* which, in turn, allows security incident response teams to *eradicate*, *recover* and then, potentially, provide *feedback* information into the next preparation stage. The final phase within many security incident response approaches is the feedback/follow-up phase (Mitropoulos

* Corresponding author.
E-mail addresses: grisposg@acm.org (G. Grispos), bglisson@southalabama.edu (W.B. Glisson), timothy.storer@glasgow.ac.uk (T. Storer).

http://dx.doi.org/10.1016/j.diin.2017.07.006
1742-2876/

et al., 2006; Northcutt, 2001). Information collected during an investigation is used in this phase to learn wider lessons from the security incident, with the aim of preventing a reoccurrence of the incident (He, 2014; Mitropoulos et al., 2006). Incident learning is usually accomplished through a series of formal reports, meetings and presentations to management (Northcutt, 2001). Lessons learned can include actions taken during the investigation, enhancing existing security controls and identifying modifications to security incident response processes (Mitropoulos et al., 2006).

Although security incident response approaches stress the importance of incident learning, researchers have observed that many organizations find it difficult to learn from security incidents (Ahmad et al., 2012; Shedden et al., 2010, 2011). A contributing factor is that although many incident response approaches incorporate a feedback/follow-up phase, these approaches provide very little practical information about the tools or the techniques that can be used to extract lessons learned from an investigation (He et al., 2014). As a result, organizations tend to focus on improving technical controls and do not reassess the effectiveness of internal policies and procedures, which could also have contributed to the incident or obstructed investigative efforts (He et al., 2014). Moreover, if an organization does extract lessons learned from an investigation, there is currently very limited tool or technique support for organizations to evaluate if these enhancements have actually been implemented in the wider organization (Grispos, 2016).

Retrospectives are an agile practice commonly used by software development teams (Derby et al., 2006). The purpose of a retrospective is to provide a lightweight approach to identify what worked and what did not work during the previous development iteration and use this information to reflect on and improve the processes used by the development team (Derby et al., 2006; Pham, 2011). In fact, previous research supports the idea that retrospectives can have a positive effect on agile development processes improvement (Maham, 2008; McHugh et al., 2012; Tiwari and Alikhan, 2011). This information prompted the hypothesis that *integrating lightweight agile retrospectives, in a security incident response environment, will enhance feedback and/or follow-up efforts*. In order to address the hypothesis, the following research questions were identified:

1. What components of a retrospective need to be modified for use in security incident response?
2. Do retrospectives assist with identifying and documenting additional information about a security investigation that, otherwise, may not be documented within a corresponding investigation record?
3. Do retrospectives assist a security incident response team in identifying and documenting security controls?
4. Do retrospectives assist a security incident response team in identifying and documenting security incident response-related process changes?
5. To what extent can a meta−retrospective highlight how many security controls and security incident response-related process changes are actually implemented within an organization?

Hence, this work investigates the impact of integrating lightweight agile retrospectives into a security incident response environment with the aim of implementing a process of on-going and incremental improvement. In addition to implementing retrospectives in a security incident response environment, a retrospective of retrospectives (hereafter referred to as a *meta−retrospective*) was also implemented in the same environment. The purpose of the meta− retrospective was to evaluate if any security controls and/or security incident response-related process improvements, identified during a retrospective, were actually implemented within an organization. The research contribution of this paper is twofold. First, it presents an approach based on lightweight retrospectives as a means of enhancing security incident response follow-up efforts. Second, it presents an empirical evaluation of this lightweight approach in a Fortune 500 Financial organization's security incident response team. The results of this evaluation indicate that it is a plausible solution for driving the development of lessons learned in security incident response.

Highlights of the retrospective/meta-retrospective implementation in this case study involving the Fortune 500 organization revealed:

- In one hundred forty-eight (148) out of the three hundred and twenty four (324) retrospectives conducted, more information was revealed when compared with the corresponding record of the actual investigation (see Table 5 for further details). This indicates that more relevant information is often available, which can be identified and documented through further reflection and consideration.
- Security incident handlers in an organization need to communicate with a wide range of individuals internally and externally (see Section Retrospectives for details). This finding suggests the importance of up-to-date contact lists, alternative contact mechanisms (potentially out-of-band channels) and a routinized way to document who was contacted and what was discussed or decided.
- In twenty-five (25) out of the three hundred and twenty-four (324) retrospectives conducted, a single security control could have prevented a security event/incident from occurring. In four (4) other retrospectives, two security controls could have prevented the security event/incident from occurring. See Table 3 and associated discussion for further details.
- The retrospectives implementation also revealed that process changes were required and, in certain cases, that completely new processes needed to be developed to assist incident handlers investigating similar future security events/incidents.
- Security incident handlers lost opportunities to investigate because relevant data sources were not always preserved (for example, Lotus Notes email, virtual machines) for a variety of reasons. This indicates a need for improved communication and coordination when an incident occurs, and for improved processes to 'freeze' relevant data sources.
- The meta-retrospectives implementation revealed that forty-two (42) out of the sixty-five (65) potential improvements identified using the retrospectives were implemented. However, the meta-retrospectives also identified that fifteen (15) out of the sixty-five (65) recommendations could not be made until they were escalated to senior management within the Information Security unit. See Table 4 for more details.
- Six (6) out of the sixty-five (65) security control and process changes identified in the retrospectives resulted in 'No Changes' being made within the organization. This is largely because the organization's security incident response team does not have authority over all the processes within the organization.

Overall, those involved in the retrospective implementation perceived the following benefits/advantages:

- That additional information was captured through the retrospectives, including information regarding data sources, contact information, and process changes/improvements.
- The retrospectives provided a 'safety-net mechanism' to help document security control modifications. They also assisted with the identification of important stakeholders whose