COMPUTER LAW & SECURITY REVIEW 34 (2018) 908–911

Available online at www.sciencedirect.com

ScienceDirect

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

Computer Law & Security Review

An approach to minimizing legal and reputational risk in Red Team hacking exercises

*Joseph V. DeMarco**

DeVore & DeMarco, LLP, New York, NY, USA

ARTICLE INFO

Article history:

Keywords:
Data protection
Data security
Cybercrime
Cybersecurity
Cyber-resilience
Computer intrusions
Ethical hacking
Network and information security
Penetration Testing
Red Team

ABSTRACT

Robust cyber-resilience depends on sound technical controls and testing of those controls in combination with rigorous cyber-security policies and practices. Increasingly, corporations and other organizations are seeking to test all of these, using methods more sophisticated than mere network penetration testing or other technical audit operations. More sophisticated organizations are also conducting so-called "Red Team" exercises, in which the organization tasks a small team of highly skilled and trained individuals to try to gain unauthorized access to physical and logical company assets and information. While such operations can have real value, they must be planned and conducted with great care in order to avoid violating the law or creating undue risk and reputational harm to the organization. This article explores these sometimes tricky issues, and offers practical risk-based guidance for organizations contemplating these types of exercises.

1. Introduction

As the amount and variety of data being stored has increased exponentially over the years, so have the challenges in keeping it safe. As a result, information security professionals have needed constantly to re-invent how to proactively test and assess the physical and technical vulnerabilities of company systems, so much so that the defenses themselves raise legal and reputational risks. "Red Team" operations conduct internal physical and logical testing to determine whether unknown vulnerabilities exist at a corporation,[1] which would permit unauthorized access to company data and systems, often without any warning to internal security personnel. This article discusses the risks of trying to break into your own network and to hack your own data.

2. The Red Team operation

Red Teaming is a form of "ethical hacking" which involves the use of techniques and methods similar to those of a criminal hacker or state-sponsored organizations to simulate a real cyber-attack (often paired with a physical intrusion) so that the corporation can learn about weaknesses in their defenses. The theory is that by simulating an attack, the Corporation

* Corresponding author: Partner, DeVore & DeMarco, LLP, New York, NY, USA.
E-mail address: jvd@devoredemarco.com

[1] Although governmental entities and NGOs can also benefit from Red Team testing, this article focuses on the issues implicated when a private corporation or similar private-sector entity conducts such operations.

https://doi.org/10.1016/j.clsr.2018.05.033
0267-3649/

can prompt appropriate changes and security improvements based on observed cyber-weaknesses. As readers of this publication are likely aware, one common example of ethical hacking is the penetration test, whereby a Company enlists a technology consultant to test certain points of vulnerability in the company's system at a certain period in time in coordination with the Company's IT personnel. In contrast, Red Teaming involves a more comprehensive cyber-security assessment of a company, often over a longer period of time and usually with little or no warning to employees within the company. Indeed, knowledge of the exercise is sometimes limited only to a handful of senior management – and in some cases, to increase the realism of the test, the CISO and head of physical security (or their functional equivalents) are deliberately *excluded* from the "circle of trust" and have no knowledge of the exercise until it is concluded.

Typically, the operation aims to identify both the cyber and physical vulnerabilities in a Company's network and systems. The Red Team (which is carefully selected and operates under strict supervision) often begins by gathering as much information as possible from publicly available sources about the "target" whether it is the corporation as a whole or a division or even single facility of the Company. This "reconnaissance phase" can also include the collection of information on Corporate personnel who will be targeted. Often, those employees' social media profiles are a rich source of data that can be used to learn who to target in order to gain access to company facilities, systems, or confidential information. The Red Team generally does not leverage knowledge of internal operations, sources of information, Corporate network access; rather, they seek to emulate access and availability of an external attacker. Once potential weaknesses are identified, the Team then employs many of the same tools that a black hat hacker would use to compromise company servers and networks, including "social engineering"[2] techniques that solicit critical information from employees under false pretenses. In addition, physical intrusion testers may be tasked with surreptitiously gaining access to areas in Company facilities to identify weaknesses in physical security or, place a device on the Company's system to aid the hacking. For example, a tester may pose as a package delivery person or use a cloned building access card to get access to a server room, or just to computers that are unattended. They may even scatter "infected" thumb drives in company offices in the hope that someone might plug them into a corporate computer.[3]

The Team may or may not provide some limited information to the company's IT department in advance for certain parts of the operation. Black Box testing is when the Company provides no information prior to the start of testing to the Team about the company's network and the Company's network defense organization has no prior knowledge of the test. Grey Box testing is when the Company provides partial details of the target systems and the network defense organization may have some notice of the test. White Box testing is when a Company provides the Team with full and complete details of the network, applications, and internal procedures and when the Company's network defense organization knows about the test in advance. The recommendations below are generally applicable to all of these scenarios.

3. Legal risks

3.1. *Access to sensitive information*

Even though the Company voluntarily authorizes[4] the hacking, it does not mean that the hacking is free of a variety of statutory and contractual legal risks. The Company's systems likely contain a variety of personal information that is subject to local and foreign national laws (and both federal and state laws in the United States). For example, in the U.S., under federal and state data breach statutes, Companies who hold personal information that is inadvertently exposed must undertake an extensive investigation and expensive remedial measures to inform affected individuals of the breach. Additionally, the exposure or deletion of data may give rise to causes of action in tort or could violate contractual provisions between the Company and third parties. A properly conceived Red Team operation should, through knowledgeable legal counsel, analyze these laws in advance, so as not to trigger a "false alarm" and needless data breach report by the Corporation.

Red Team operatives should, to the extent possible, avoid viewing any electronic financial data, credit reports, employee or applicant data, or health data. Unless otherwise stated in writing, data exfiltration relating to employees—whether current, former, or prospective—of the Corporation should almost always be prohibited or only be conducted with prior approval and appropriate documentation. Similarly, exfiltration of data outside of the internal network should not be permitted. In addition, to maximize security, information compromised during a testing engagement should not traverse the internal network with risk of external exposure. Moreover, unless otherwise approved in advance, testers should not access or attempt to access customer data, sensitive employee information, or systems housing information not owned by the Company.

In terms of attack technique and tradecraft, malware should never be employed for any purpose during the exercise. In addition to implicating potential liability under local computer crime laws, the malware may damage data or spread to other systems in unpredictable ways that could give rise to a claim sounding in negligence, among other legal liabilities.

[2] Examples of "social engineering" include sending phishing emails to Company employees or "pre-texting," communicating with employees using a fabricated scenario to obtain information.

[3] Naturally, the drives will not contain any actual malware; they can, however, be configured to "beacon home" to the Red Team operations center with information about where the drive was connected and, potentially, who connected it. Targeted remedial measures can then be considered by management.

[4] As will be discussed elsewhere, see infra, it is crucial that internal or external legal counsel versed in the issues discussed herein be closely involved in the conceptualization and execution of the exercise. At the outset, counsel can guide the Corporation in the proper methods of exercise authorization so as to ensure that it is not "ultra vires" while at the same time maintaining the parameters of desired secrecy.