Cyber Security in Banking Sector

Michael BEST[1], Lachezar KRUMOV[2], Ioan C. BACIVAROV[3]
[1] Auditor for Cyber Security, Deutsche Bank's Group Audit Department, Frankfurt, Germany and PhD Student, University "Politehnica" of Bucharest, Romania
mb@michael-best.de
[2] PhD, Auditor for Anti Financial Crime, Deutsche Bank's Group Audit Department, Frankfurt, Germany
[3] Professor, PhD, Director of EUROQUALROM - ETTI, University "Politehnica" of Bucharest, Romania, President of RAISA
ibacivarov@yahoo.com

Abstract

Because banks are very often target of a cyber-attack, they have also good security controls in place. This paper analysis modern threats to banks and proposes an approach to detect and visualize the risk of data leakage. In the first part of this paper, a comparative analysis of the most common threats to the banking sector is made, based on both bank reports and cyber security companies. The authors came to the conclusion that at the bottom line, insider knowledge is necessary, which is the result of data leakage. This paper comparatively analysis modern threats to banks and shows an approach to detect and visualize the risk of data leakage. In the second part of the paper, a model - based on network graph - that can enumerate the risk of data leakage is proposed. Graphing a network of an organization with the connections of data flow between assets and actors can identify insecure connections that may lead to data leakage. As is demonstrated in this paper, financial institutions are important targets of cyber attacks. Consequently, the financial sector must invest heavily in cybersecurity and find the best ways to counter cyber attacks and cyber bank robbery attempts.

Index terms: Security, Bank, Cyber-Security, Financial Threats, Information Leakage Prevention, Information Leakage Model

References:

[1]. New York Times, 2016, https://www.nytimes.com/2016/05/01/business/dealbook/hackers-81-million-sneak-attack-on-world-banking.html.

[2]. Reuters, 2016, https://www.reuters.com/article/us-cyber-heist-philippines/bangladesh-bank-officials-computer-was-hacked-to-carry-out-81-million-heist-diplomat-idUSKCN0YA0CH.

[3]. BAE Systems Research Blog, 2016, http://baesystemsai.blogspot.de/2016/04/two-bytes-to-951m.html.

[4]. Bankinfosecurity 2016, https://www.bankinfosecurity.com/bangladesh-bank-heist-probe-finds-negligent-insiders-a-9586.

[5]. Intel Security, Data exfiltration study: Actors, tactics, and detection, 2015.

[6]. Avast, 2017, https://blog.avast.com/mobile-banking-trojan-sneaks-into-google-play-targeting-wells-fargo-chase-and-citibank-customers.

[7]. T. Cormen, C. Leiserson, and R. Rivest, Introduction to Algorithms, Cambridge, MIT Press.

[8]. M.Alexander, Methods for Understanding and Reducing Social Engineering Attacks, 2016, https://www.sans.org/reading-room/whitepapers/engineering/methods-understanding-reducing-social-engineering-attacks-36972

[9]. Symantec Corporation, Financial Threats Review, 2017, https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-financial-threats-review-2017-en.pdf.

[10]. M. Best, A Graph Driven Approach to Data Leakage Prevention, 2017.

[11]. W. Stallings, and L. Brown, Computer Security - Principles and Practice. 3. s.l, Pearson, 2015, 9781292066172.

[12]. Lehtinen & Lonvick, The SSH-Protocol, https://tools.ietf.org/html/rfc4250.

[13]. Rescorla: HTTP over TLS, https://tools.ietf.org/html/rfc2818.

[14]. Information Sciences Institute, University of Southern California, TCP, https://tools.ietf.org/html/rfc793.

[15]. OWASP, OWASP Risk Rating Methodology. [Online] [Cited: 07 14, 2017], https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

[16]. E. Snowden [Cited: 03 25, 2018], https://www.nytimes.com/2014/01/02/opinion/edward-snowden-whistle-blower.html.

[17]. C. Manning [Cited: 03.25, 2018] New York Magazine, http://nymag.com/news/features/bradley-manning-2011-7/.

[18]. I. Bacivarov, A Regional Strategy for Cybersecurity, International Journal of Information Security and Cybercrime, Volume 4 (2015), Issue 1, pp. 5-8, ISSN: 2285-9225.