leviathan security group

Leviathan Security Group, Inc.
3223 3rd Ave S., Suite 100
Seattle, WA 98134

SaneBox, Inc.
13920 NW Passage
Suite 209
Marina del Rey, CA 90292
October 15, 2019

To: Dmitri Leonov
Senior Vice President
SaneBox, Inc.
RE: Google Project ID: sanebox-01

On September 24th, 2019 Leviathan Security Group conducted a limited penetration test and document review of the SaneBox application produced by SaneBox. We assessed the application, supporting infrastructure and SaneBox answers in a self-assessment questionnaire.

Leviathan verified the application’s use of the following **restricted** Google API scopes:

https://mail.google.com/ (includes any usage of REST, IMAP, SMTP, and POP3 protocols)

https://www.googleapis.com/auth/gmail.readonly

https://www.googleapis.com/auth/gmail.metadata

https://www.googleapis.com/auth/gmail.modify

https://www.googleapis.com/auth/gmail.insert

https://www.googleapis.com/auth/gmail.compose

https://www.googleapis.com/auth/gmail.settings.basic

https://www.googleapis.com/auth/gmail.settings.sharing

Leviathan verified the application’s use of the following sensitive Google API scopes:

https://www.googleapis.com/auth/drive

This testing was undertaken as a part of the Google Cloud Platform OAuth API Verification and should not be read as a comprehensive penetration test or maturity assessment. The purpose of the engagement was to identify security issues with SaneBox’s application and infrastructure during the time allocated to us. Leviathan used automated and manual testing as well as review of the Self-Assessment Questionnaire filled out by SaneBox and associated documentation.

This letter confirms that the testing of the SaneBox application and supporting infrastructure has been completed and that all issues with a Critical or High-risk finding have been remediated. SaneBox's management has received a report with detailed findings and recommendations from this engagement.

The testing followed the requirements as described in the OAuth API Verification FAQ as last updated on September 16, 2019. These requirements are detailed in Appendix A at the end of this letter. This letter is valid for up to 12 months from the issue date.

Signed,

Robert Bregant II

Bob Bregant
Director, Risk and Advisory Services
Leviathan Security Group

Appendix A

1. *External Network Penetration Testing: Identify potential vulnerabilities in external, internet-facing infrastructure, systems such as the following:*
    - *Discovery and enumeration of live hosts, open ports, services, unpatched software, administration interfaces, authentication endpoints lacking MFA, and other external-facing assets*
    - *Automated vulnerability scanning combined with manual validation*
    - *Brute-forcing of authentication endpoints, directory listings, and other external assets*
    - *Analysis of potential vulnerabilities to validate and develop complex attack chaining patterns and custom exploits*
    - *Potential exploitation of software vulnerabilities, insecure configurations, and design flaws*
2. *Application Penetration Testing: Identify potential vulnerabilities in application that access Google user data such as the following:*
    - *Real-world attack simulation focused on identification and exploitation*
    - *Discovery of attack surface, authorization bypass, and input validation issues*
    - *Automated vulnerability scanning combined with manual validation*
    - *Exploitation of software vulnerabilities, insecure configurations, design flaws, and weak authentication*
    - *Analysis of vulnerabilities to validate and develop complex attack chaining patterns and custom exploits*
    - *Verify the ability for users to delete their account with no external indication that the user or user's content is accessible.*
3. *Deployment Review: Identify exploits and vulnerabilities in developer infrastructure such as the following:*
    - *Gathering all available configuration settings and metadata as well as manual techniques to build a profile of the cloud environment*
    - *Analyzing collected information to identify any gaps or deviations from accepted cloud security best practices*
    - *Manually examining configuration settings to locate anomalies and issues such as weak IAM policies, exposed storage containers, poorly defined security groups, insecure cloud services usage, and insecure key management*
    - *Exploitation of vulnerabilities, insecure configurations, design flaws, and weak authentication – as needed*
    - *Verify storage of OAuth tokens is encrypted and encryption keys and secrets are stored in a hardware security module or equivalent strength key manager*
    - *Ensure developer access to the deployment environment is secured with multi-factor authentication*
4. *Policy and Procedure Review: Review and examine the efficacy of information security policies and procedures such as the following:*

- *Incident Response Plan: Establishes roles, responsibilities, and actions when an incident occurs*
- *Risk Management Policy: Identifies, reduces, and prevents undesirable incidents or outcomes*
- *Vulnerability Disclosure Program: Provides a means for external parties to report vulnerabilities*
- *Information Security Policy: Ensures that all users comply with rules and guidelines related to the security of the information stored digitally at any point in the network*
- *Privacy User Data Detection: Ensures that users can delete their accounts and related user data by demonstrating an account deletion if relevant*