SaneBox Security and Privacy Overview

We realize that email contains our customers' sensitive private data, so we take security and privacy of our user data seriously. We adopt a four-tiered approach to email security.

I. Network Security

The service and database machines do not accept any connections from the public Internet. A SaneBox employee must establish a VPN connection to our private network.

The employee is required to provide individual cryptographically strong SSH keys to gain access to a bastion host. Once connected to the bastion host, the employee has to provide SSH keys to gain access to one of the service machines. All such access is logged and routinely audited. Finally, all data on the server is secured with bank-quality encryption.

II. Data Security

By design, emails never reside on our servers. Our software cannot see the content of user's emails, since the body of emails will never touch our servers. The servers that calculate the importance of emails and label them are unavailable for inbound connections from the public Internet.

Additionally, SaneBox acts as a client so that if our service should be down for a brief period (we aim for 5 9's of uptime), user email delivery will continue, and unimportant email will continue to funnel into the Inbox until service resumes.

User's email authentication credentials are bank-quality encrypted via industry best practices. They are encrypted via Blowfish CBC with a cryptographically secure randomized 8-byte initialization vector.

User's SaneBox password is hashed in the database, also using industry best practices. They are salted and hashed using 500 iterations of SHA256 via a NIST-approved PBKDF2 algorithm. An industrial strength passcode must be entered to start up the software. Even in the worst case scenario - someone walking off with the entire database and the entire source code - they would still not get access to a single authentication credential. This master startup passcode is known to only a few trusted employees.

III. Physical security

We co-locate in hardened facilities in secure racks. The data centers are housed in nondescript facilities and have extensive setback and military grade perimeter control as well as other natural boundary protection.

Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state of the art intrusion detection systems and other electronic means.

IV. Trusted Personnel

SaneBox Inc. maintains a detailed internal security policy issued to all employees and reviewed frequently. We only hire people who come highly recommended and referred by our trusted contacts, after performing extensive reference checks.

Employees are provided with security training as part of new hire orientation. SaneBox provides confidential reporting mechanisms to ensure that employees can anonymously report any ethics violation they may witness. Hence, it is the most vetted subset of our trusted employees that even access that final encryption key.

V. SaneBox Network Security Diagram