LiveBox

2014

LBSEC

LiveBox Srl does not release declarations or guarantee regarding this documentation and its use and declines any expressed or implied commercial or suitability guarantee for a specific purpose. LiveBox Srl reserves the right to review this publication and to make changes to the content, anytime, without any obligation to notify it to any person or entity about that revisions or changes.

In addition, LiveBox Srl does not release declarations or guarantees about any software e in particular does not recognise any expressed or implied commercial or suitable guarantee for a specific purpose. LiveBox Srl reserves the right to review this publication and to make changes to any LiveBox software part, anytime, without any obligation to notify any person or entity about said revisions or changes.

LiveBox is a private cloud software that allows you to store, share and edit data stored in a corporate datacenter offering a high security level. It is a multiplatform system accessibile from any mobile and remote device that guarantees business continuity and protects corporate files at all times.

For further details regarding LiveBox platform functionality and the use of its applications we ask you to refer to our web site: http://www.liveboxcloud.com and to the technical documentation contained in it.

LiveBox Support Team

LiveBox

Index

1. LIVEBOX, A PRIVATE FILE SHARING

LiveBox is a private file sharing platform with a client/server architecture. The server is located within the customer infrastructure, ensuring privacy and security of the data.

Having an internet connection with public IP (or recorded on a dynamic naming service) it is possible to guarantee remote accessibility. It can be realized from standard compatible browsers HTML5 (IE 10, Firefox, Chrome, Opera, Safari), from OS Android systems (4.x), from iOS systems (from 6.x), from Windows systems (from XP SP3, 32 bit or 64 bit), from Mac OSX (>= 10.7). During 2014 will ensure the platform support Windows Phone 8.

Two paradigms lead our development platform:

- Installation and use inside your own hardware infrastructure.
- Sharing contents, in a private and secure way, without files relocation.

2. SECURITY

Usually LiveBox organizes his security divided in two areas:

1) Transport protocol security:

   HTTPS protocol performes secure transactions between client and server, through Intranet or Internet communications. Data is encrypted by the server before transfer, this is achieved using a protected communication channel established through a web certificate.

2) Data security:

   Data location: Data is located in the client's infrastructure, so its informations are saved on the client's repository. This guarantees that corporate data is always located inside the corporate infrastructure, providing tracing systems and data leak prevention.

   Encrypted data: Content data is encrypted, using a PIN Code chosen by the user during first login on the platform, this PIN is known only to the final user and does not reside on the server platform. Data is saved on the mobile device encrypted with AES 256 symmetrical encryption, also using the hash of the PIN code chosen by the user. The symmetrical key encryption allows a fast encryption and decryption data, ensuring computing power friendly access for both the client and server.

   Asymmetrical key privacy: Data on the user's disk is encrypted using the PIN Code, preventing users with administrative permissions or root users from accessing the data. LiveBox user's device allows to separate data encryption from the security of the operating system hosting of the application.

2.1 REMOTE WIPE

The system allows system admins of LiveBox applications to disable access from a pre authorized device. In this way is possible to disable the access to the data for remote users with expired authorization or to disable access on stolen or lost devices.

2.2 PENETRATION TEST

The LiveBox system has passed the penetration tests of the top 10 Oswap 2013 (Open Web Application Security Project), with the following results:

Injection (A1)	No alerts in this category
Broken Authentication and Session Management	No alerts in this category
Cross Site Scripting (XSS) (A3)	No alerts in this category
Insecure Direct Object Reference (A4)	No alerts in this category
Unvalidated Redirects and Forwards (A10)	No alerts in this category

This analysis has been performed using Acunetix v.8 a specialized commercial software for penetration testing on web applications.

2.3 SECURE CODE (NO REVERSE ENGINEERING)

LiveBox application code is encrypted, this is done to prevent reverse engineering of the application by an OS admin user or a spiteful user.

2.4 PIN USE

The PIN, within LiveBox system, corresponds to the user's private key. The user can encrypt or decrypt his files, in a selective way using this PIN code. This operation does not prevent sharing encrypted files with other users.

2.5 HTTPS PROTOCOL

HTTPS protocol is utilized to encrypt transport data from the device through which the user can login on the Livebox system, independently from the intermediate network path, preventing data tampering, falsification, and interception.

The HTTPS protocol used in Livebox is characterized by an SSL (Secure Socket Layer) cryptography system with unilateral TLS. This is the web-server that authenticates on client, upon first login. LiveBox uses cookies to provide advanced functionality on the LiveBox web portal, the user has to accept Cookie Use during the first login access from a browser, this also enables two-step authentication for added security. The cookie is used during first access (user credentials). As soon as the Pin is set, this is used only by previously authorized devices to enable chat sessions in a secure and privacy oriented environment.

The authentication is divided into four levels:

- Server authentication on client (trasport-network level): the client verifies the server's identity through the web certificate, authorization is granted by a class 1 Certification Authority already installed in the root certificate of the user's browser. The SSL session on the web server ensures that the transport between client and server is protected on the network level.
- User authentication (user-network level): the user enters credentials (local or on server remote LDAP/AD) to download the application; Livebox server contacts it's internal DB (if the user is a local one) or LDAP remote server, through a LAN connection, using the LDAP proxy reverse role (without compromising the local password or user domain).
- Cookie authentication (application – device level): once a user's device is correctly authenticated it releases a cookie that certifies the connection with Livebox server. The session is authenticated by the application server layer in order to verify that the user's connection device was previously authorized with a previous successful login.
- PIN authentication (applicative - user level): the LiveBox application on the device is unlocked using the user's PIN code, a hash of this PIN code is used to encrypt data transfers to the application level and on the local file system.

2.6 ANTIVIRUS

LiveBox system is secure against content alteration and from operating system file modifications, this is achieved by preventing execution of suspicious files.

An additional protection level from the effects of virus infections is depends on files being locally saved in the disk space without extensions. In this case, even a localized Trojan inside the server can not execute code locally through registered files, as everything is encrypted.

The system can easily be protected before an infected file is saved tothe local storage. The file passes through a common proxied protocol such as http/https, making inspection by proxy antivirus software, such as the Open Source (HVProxy) or commercial solutions like (F-Secure Proxy server, Symantec Gateway Antivirus, Firewall UTM – Fortigate Antivirus) trivial.

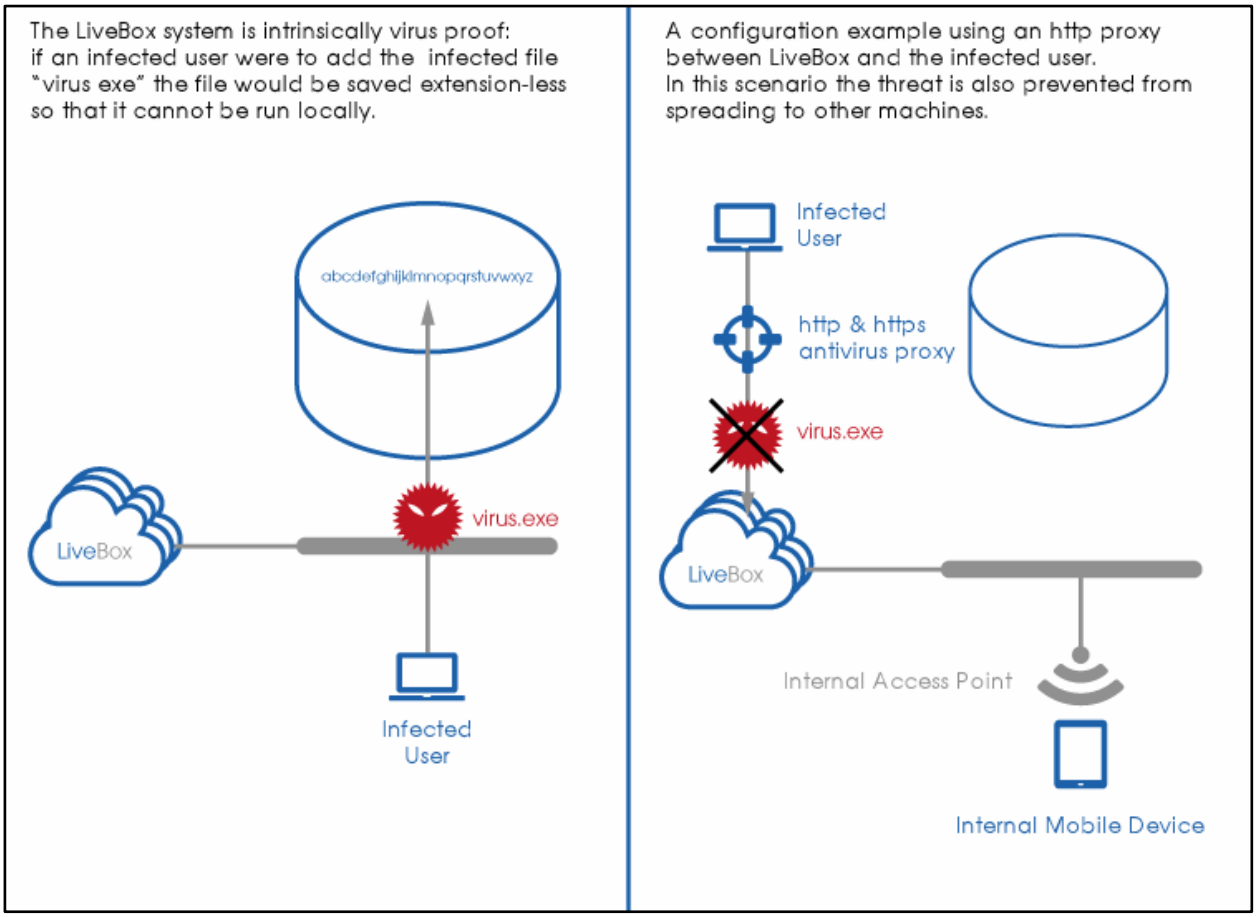

Figura 1: The LiveBox system resisting a virus infection; using a proxy Antivirus is it is possible to prevent the diffusion toward other clients.