How is the private key protected

What measures are in place to prevent server administrators or anyone else but me from accessing my private key?

As a first measure, your private key will be encrypted using a pass phrase that is only known to you. This password is not stored anywhere on our systems and needs to be entered separately after login to decode the key. Unless a user is logged in to mailbox.org your PGP key exists only in the form of a further encrypted code that cannot be used for anything.

Secondly, after login, the private key is temporarily decoded by the user entering the pass phrase, and then immediately encoded again with a separate encryption key that changes randomly with every successful login attempt. The temporary key is then sent to the browser and valid for a single session. Again, it is not stored anywhere on our systems.

As a result, neither any passwords nor the PGP key of a user is stored permanently anywhere on the harddisks or program memory of our servers.

Thirdly, OX Guard receives the temporary key from the browser of the client only when that key is actually needed to decrypt an e-mail. The software will not keep the key stored in a variable and hence, it will reside in program memory only briefly.

If a user logs out, the temporary key will be void. Even if an attacker manages to retrieve the key from your previous browser session, it will be worthless as it cannot be used again to decode the PGP key.

Suppose an attacker was able to retrieve the temporary key during its transmission to the browser, it would still be quite impossible to actually get the true PGP key because the server login required for this will instantly invalidate whatever temporary code had been previously intercepted.

However, an attacker who has physical access or local control over the web browser on the client device may be able to take over the current mailbox.org Office session and so, in principle, obtain the temporary key. Nevertheless, this key would only be of short use as it will expire once the user logs off or the browser session times out.

The previous scenario is a bit theoretical, though, as it does not really present a weakness on behalf of mailbox.org Guard. At this point, the attacker already has significant access to the device system and the web browser and hence, is very likely to also have access to the decrypted e-mails and all related file data anyway. Any potential compromise of an existing PGP installation on either the local device or the mailbox.org Guard on the server would then probably not make much of a difference anymore.

As a consequence, we can establish that maintaining the security of the local client hard- and software is a crucial element for the overall security of any communication. This part is outside of the control of mailbox.org, yet at least we can assume that using OX Guard will be unlikely to create additional vulnerabilities. One could argue that it is quite the opposite, actually: If the PGP key resides on the mailbox.org server, an attacker will still not be able to retrieve this key, while they could easily do so if it was stored directly on the client device.

Related Articles

- How to set up Mailvelope
- How can e-mails be encrypted with PGP
- Which PGP standards are supported
- The Encrypted Mailbox
- Can I trust the staff at mailbox.org