Prevent Shadow IT

How to satisfy your compliance requirements and users at the same time – while securing your digital communication.

What is shadow-IT?

The term shadow-IT describes a developing trend in business where employees use software and technologies for work that are neither implemented nor approved by IT, or the compliance-team. As this practice can lead to severe security issues companies should be aware of the risk and inform themselves on how to minimize those.

“One cannot, not communicate”. Paul Watzlawick made this remark, and whilst back then he said it in another context it can be applied in today’s business world: Today we would say “One cannot, not communicate digitally.” Most communication in companies is done electronically. Be it e-mail, file exchange, messaging, or social platforms. In the course of this the IT-environment becomes ever more complex and the users’ expectations increase.

From private everyday communication, staff are used to means of communication that are setting the standards for what they want to use in their business environment. If the company fails to offer tools that live up to these expectations the users eventually turn to an alternative that offers them what they want and need to stay productive with the least user hurdles. This in turn leads to the use of software that isn’t compliant to the company’s security and data protection standards – unknown by the IT-department. The result is the so called shadow-IT.

How shadow-IT comes about

A common scenario for the rise of shadow-IT is the need to exchange files: everyday someone in the company has to exchange large files with a colleague, customer or partners. Since the most usual method of communication is the e-mail, it’s the natural choice to also use it for exchanging files – as attachments to a message or just as a file transfer with a short note. Most e-mail systems however are limited to only a few megabytes per message and are not designed to store large amounts of data. For lack of an option and under time pressure users turn to what they know from their private life: Public cloud solutions like Dropbox, GoogleDrive, or iCloud are well known, quick to get started and enabled to quickly get the file exchange going with external communication partners. For the user this way the problem is quickly fixed. For the company it can have severe consequences.

befine Solutions AG
Werthmannstrasse 15
79098 Freiburg

info@cryptshare.com
Tel. +49 761 389 13 0
Fax. +49 761 389 13 115

Risks of shadow-IT

When employees use unauthorized software the company immediately loses control over files that are stored on publicly available servers outside of their own infrastructure. This can already be an infringement of laws and regulations in many industries that handle, store, and exchange sensitive data of customers, patients, or clients. In addition, many cloud services have only rudimentary 'one policy for all' security so that once an account is hacked all accounts and data are exposed – as many cases have shown in the past.

Especially with sensitive customer data and classified corporate information these consumer grade solutions are not suitable since the files are not necessarily stored and transferred encrypted.

Understanding the user

Even though employees might be used to the convenience of file sharing tools from their private life that doesn't mean companies have to tolerate the unsanctioned use of them. But instead of simply outlawing them the leadership, in cooperation with the IT-department should ensure that secure and controlled options are available that are still as convenient to use as a regular e-mail or privately known tools. Most employees only turn to unauthorized tools because there is no convenient one available – SFTP, S/MIME, and the like might cover the security requirements of a company but are outdated and just too complicated for the average business user.

Getting a solution that combines security and convenience

The needs that lie beneath the surface are to simply exchange messages and large files in an easy way and spontaneously with anyone inside or outside the company. If this is possible with a tool that is authorized by the company and even integrated in the familiar working environment, then there is no reason for the users to employ the illegitimate software. In order to adjust their IT-infrastructure to these challenges and find the right solutions companies should check the following seven points:

1. Ease of use:
   If the software is straightforward it will gain user acceptance much faster and make implementation easier.
2. Readily available:
   A solution that is always on-hand without entry barriers, such as installations or exchange of certificates, will increase productivity.
3. Suitable for all contents:
   Messages and files of all sorts and sizes should be exchangeable via the tool without any problems.
4. Good value:

befine Solutions AG
Werthmannstrasse 15
79098 Freiburg
info@cryptshare.com
Tel. +49 761 389 13 0
Fax. +49 761 389 13 115

A fair pricing model and no additional cost for external users and private customers of your company make the right solutions cost-efficient.

5. Confidential:
   Transit and temporary storage have to be encrypted.
6. Secure:
   Interfaces for antivirus scanning, Data Loss Prevention (DLP), and key management through the company are should be standard.
7. Adaptable to your compliance:
   The right software provides comprehensive logging, options for archiving, confirmation of receipt, and by this full auditability.

befine Solutions AG
Werthmannstrasse 15
79098 Freiburg

info@cryptshare.com
Tel. +49 761 389 13 0
Fax. +49 761 389 13 115