PLM IT REPORT

Reprint from No. 1 | January 2014 |

OPENDXM® GLOBALX

Secure communication

www.plm-it-business.de

PROSTEP
integrate the future

Greater data security for e-mail communication

Simple but secure: With OpenDXM GlobalX from PROSTEP, encrypted data exchange is as easy as sending an e-mail.

The case involving Edward Snowden has shown us two things: Firstly, how remiss we are when it comes to handling confidential information and secondly, how shamelessly inquisitive intelligence services exploit this fact. It's anyone's guess whether they really only use the information they extract for intelligence purposes or also for economic purposes. What is clear is that e-mail encryption alone is not enough to protect our know-how – we need protection mechanisms that are integrated in the e-mail programs themselves.

Be honest: Do you encrypt your e-mails? If you don't, you are in good company. Approximately 144 billion e-mails are sent around the world each day (1), of which roughly no more than 3 percent are encrypted. Easy prey for data thieves. The reason for this is quite simple: most users find setting up encryption much too complicated. Otherwise, how do you explain the large number of Internet sites dealing with the topic „e-mail encryption made easy"? If the proportion of encrypted e-mails is nonetheless growing, then it is because, paradoxically, spam is being encrypted to an increasing extent. According to Pingdom, spam now accounts for 68.8 percent of all e-mail traffic worldwide.

Following the most recent scandals, many users are rightly asking themselves whether encryption is even worth the effort. According to a report in the Guardian, Microsoft of all people has revealed itself to be the fox guarding the hen house, helping the NSA, America's most secret of intelligence services, to circumvent the encryption of data by those using its services (2). As if MS Outlook didn't already have (hadn't already had) enough gaps in security – several years ago, even the German Federal Office for Information Security felt compelled to issue a warning about using the American software giant's e-mail programs (3). That has not done MS Outlook's popularity any harm.

Irrespective of all safety concerns, it is impossible to imagine our working lives without Outlook & Co. According to a study conducted by the Fraunhofer IPK together with CONTACT Software and the VDI, even engineers, who should actually be undertaking more creative work, spend more time on communication and coordinating development projects than on their core tasks (4). Their most important IT tool is therefore not the CAD system but rather the e-mail program, which many of them still use to exchange sensitive information such as CAD and product data as well as key business figures despite the strict security measures in place in the companies.

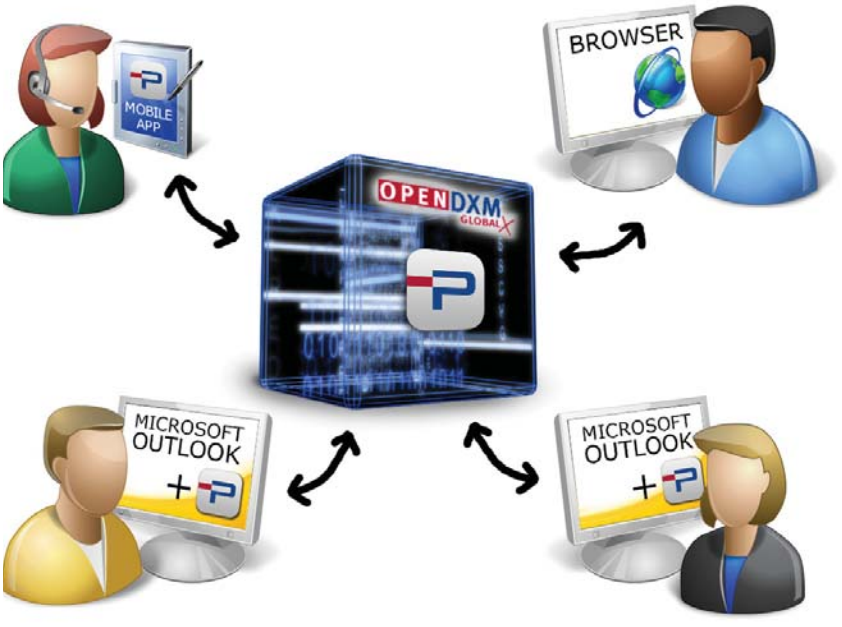
Simple solution required

What many users might not know is that even encrypting e-mails will not provide sufficient protection for their intellectual property. The encryption mechanisms included in e-mail programs normally only encrypt the e-mail body but not the attachments, which often contain confidential information. This not only applies to CAD data, which is full of design know-how well worth protecting, but also to sensitive simulation data (e.g. from crash tests) or copyright protected graphic, image, music and video files. These files often reach a size that would bring any e-mail program to its knees, i.e. it is either impossible to send them as an attachment, or they can only be sent distributed over multiple e-mails.

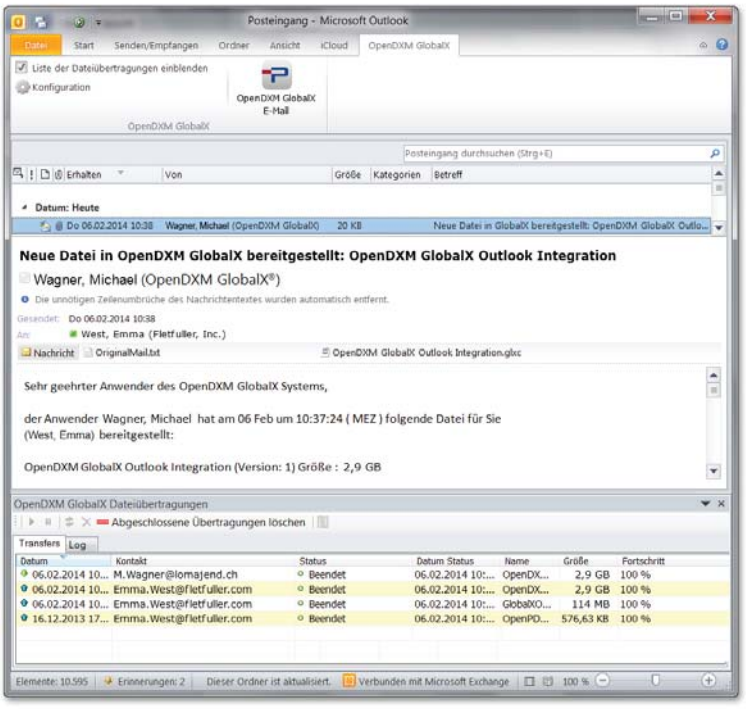
You have to wonder why even at larger companies so much data is still being exchanged without any security measures whatsoever. Probably because things usually have to be done quickly, and all the other mechanisms are more complicated to use than the e-mail program that all of us can use in our sleep. Therefore, a key requirement for any secure data exchange solution is that you can use it just as easily as you do your e-mail program. Or better yet, you use it exactly like you do your e-mail program. This is a requirement that PROSTEP AG intends to meet with its new OpenDXM GlobalX Outlook integration component.

Fully integrated in MS Outlook

From the users' point of view, the data exchange client is fully integrated in the Outlook user interface. The only difference is two additional buttons, one for sending large files and the other for forcing files of any size to be sent via OpenDXM GlobalX. The first function is actually redundant since the rules of



OpenDXM GlobalX allows flexible use while remaining highly secure.



With OpenDXM GlobalX from PROSTEP, encrypted data exchange is as easy as sending an e-mail.

the data exchange platform specify that once data exceeds a certain volume, it is automatically exchanged via OpenDXM GlobalX. The problem is that Outlook's standard „Attach File" function needs several minutes to determine that a file containing multiple gigabytes of data is much too big to send by normal e-mail. Users can overcome this obstacle with the „Attach Large File" function.

But the OpenDXM GlobalX Outlook integration cannot only be used to automatically „redirect" files that exceed a certain size to the data exchange platform. The system administrator can with little effort define rules, for example that files with a certain extension are always to be sent via OpenDXM GlobalX, i.e. are to be sent in encrypted form. Or files being sent to people in countries that are not so strict when it comes to know-how protection. Thanks to the second button, users also have the option of using OpenDXM GlobalX to send any file to any user, even if none of the defined rules automatically applies.

Activating spontaneous recipients

From the recipient's point of view, downloading the data will vary depending on whether or not he is also using the OpenDXM GlobalX Outlook integration. In either case, he will be notified that data is available for download. This message can include the body of the original e-mail or not – depending how the company involved has configured the solution. If the recipient is not using an Outlook integration, he will have to log on to the OpenDXM GlobalX portal, which opens automatically when the link in the message is clicked, using his password to access the download. If he is also working with the OpenDXM GlobalX Outlook integration, downloading is even easier – all he needs to do is click on the file attachment in the OpenDXM GlobalX message; he can then download and save the file as usual using Outlook. In this case, additional authentication on the OpenDXM GlobalX portal is not necessary.

An interesting question is what happens if the user sends files to a recipient who is not yet known in the OpenDXM GlobalX database. A company can define a uniform template for this spontaneous, or ad hoc, exchange process which automatically generates a temporary account, possibly with restricted user rights, for the recipient. In this case, the recipient not only receives a message about the data that is available for downloading but also two other e-mails: one containing his user ID and a second containing a temporary activation link prompting him to specify a password for access to the portal.

The solution is so flexible that it is even possible to define personal encryption with a public and a private key ad hoc. In this case, the files are encrypted using recipient's public key. The recipient is the only person who possesses the private key needed to decrypt them. A wizard will help him generate the private key during the course of an online session. The applet prompts him to define what is referred to as a „keystore" and specify where the private key is to be stored, for example on a USB flash drive. It also prompts him to protect access to the keystore with a separate password. Personal encryption using keys of up to 4096 bits ensures the highest possible level of data security.

Secure data exchange platform

OpenDXM GlobalX is a highly secure data exchange platform that is normally set up by the company who owns of the collaboration projects; but it can also be hosted by PROSTEP AG or another provider. It is normally installed in what is referred to as the „demilitarized zone", i.e. between the internal and external firewalls of the company in question on a central server to which only system administrators have access, which allow them to define the profiles for the exchange partners and the rules for the data

Highest possible level of data security even when exchanging data with Outlook.

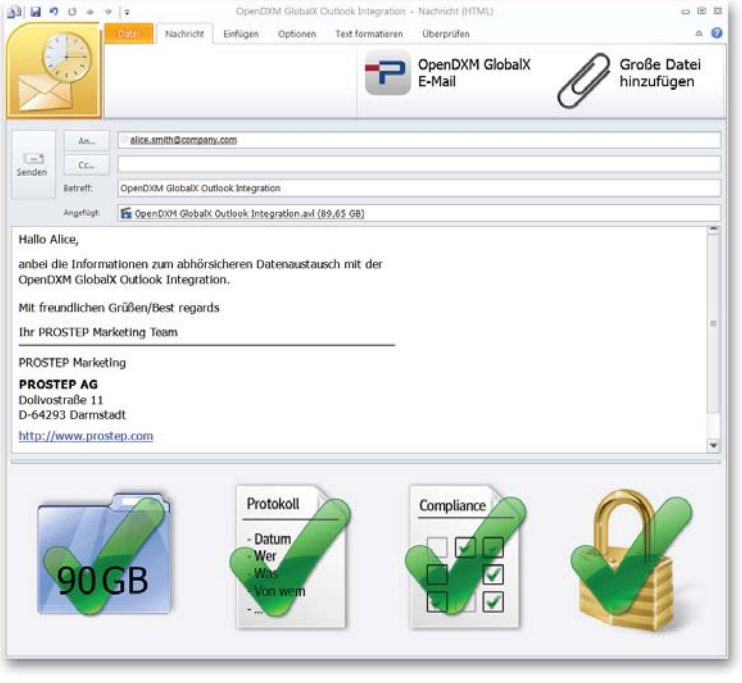
exchange process. In addition, the encryption mechanisms are stored on the server, which also performs any necessary processing, such as virus checks, forwarding data to backend systems or data conversion.

The data, which is encrypted at all times, can be placed in an OpenDXM GlobalX FileVault on decentralized servers to optimize data traffic over large distances. This means, for example, that the American subsidiary of a German company makes the data available to a project partner in the USA locally even though the partner has to log on to the central server in Germany in order to download the data. This architecture offers the advantage that the OpenDXM GlobalX server can be operated in a country with strict data protection regulations, where intelligence agencies cannot simply demand that the keys be handed over – as is the case in the USA, for example. Without the keys, the encrypted data in the remote FileVaults is of no use to them.

The data to be exchanged is encrypted using public-private key encryption when it is uploaded to the platform. In the case of normal encryption, OpenDXM GlobalX is the master of the public and the private key and ensures that the data is automatically decrypted when it is downloaded so that the authorized recipient can read it. If, on the other hand, the person sending the data decides to use personal encryption, the recipient must have a private key to which only he has access in order to read it. In this case, the intelligence services would have to devote even more time to cracking the encryption since they will need the private key to do this and it is stored password protected on the user's storage medium of choice.

Documentation of exchange operations

Sending data via the exchange platform has the additional advantage that all exchange operations are logged and can thus be used at any time for audit purposes. Although OpenDXM GlobalX does not store the



The advantages: transfer of very large files with Outlook, full documentation, automatic compliance with company-specific rules, highest possible level of security for confidential documents and easy operation.

attached file, it does store all the other information that belongs to each individual data exchange operation. When using the OpenDXM GlobalX integration, even the text body of the original e-mail is also archived. The text body is not stored as a document but written directly to the database instead, thus making it possible to perform full-text searches according to sender, recipient, subject or other search criteria. The user, of course, only sees the e-mails that he himself has received or sent via OpenDXM GlobalX – a group leader or system administrator, on the other hand, have an overview of all the exchange operations for a certain project.

The integration of the data exchange platform OpenDXM GlobalX in MS Outlook not only provides the highest possible level of data security and protection for file attachments but also allows the exchange operations to be traced at all times.

The OpenDXM GlobalX Outlook integration is now available.

Acceptance of the solution depends largely on the fact that it is actually invisible to the end user. The ability to define uniform, enterprise-wide rules for handling sensitive data is in case of doubt and in the long run more important than getting the better of the data spies at the NSA and Co.

(1) see http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers

(2) see www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

(3) www.welt.de/wirtschaft/webwelt/article5918620/Bundesamt-warnt-jetzt-auch-vor-Outlook.html

(4) www.ingenieur.de/Arbeit-Beruf/Management/Ingenieure-Freiraum-fuer-Engineering-Konstruktion

Michael Wendenburg, Sevilla
(www.wendenburg.net)

PROSTEP AG, Darmstadt,
Phone +49 6151 9287-0,
www.prostep.com