JAMsoftware

Contents

Save time, gain security

Email Archiving Solutions

Business life without email is next to impossible. Orders, offers, applications, confirmations – email is the number one communication highway. Businesses should treat emails as the important instruments that they are. Often, this is not the case. Let's examine email storage behavior and offer best practices.

Email Storage or Email Archive?

When talking to customers, there are some problems we hear of time and time again. The worst one: „In our company everybody stores emails the way they think is okay."

❯ Printing out emails: Wastes resources and space, is not searchable.

❯ Storing emails somewhere in Outlook: Emails are not secure, often there is a size limit for Outlook profiles in place.

❯ Storing emails in a folder on the hard disk or on external media: Customer information is unsecured, accessible by anybody - document folders are often the first place virtual intruders look for.

All those measures have three things in common: They are insecure, they might store emails, but they do not archive them.

What Defines an Email Archive?

Archiving an email means preserving it and keeping it searchable. Archived emails can be accessed easily and will not be lost. An archive should offer security against access to or tampering with the emails it contains.

Some countries set specific rules and laws regarding how emails have to be archived.

Why Should I Archive Emails?

Users have to understand that email messages are not actually stored on their computer, but on an email server like Microsoft Exchange Server.

If they never clear the messages, the Exchange server might start reacting sluggish as emails weigh it down.

Reasons for archiving email using a professional solution:

❯ Keep emails safe, even if the server is lost.

❯ Make sure that no one will be able to alter emails behind your back.

❯ Have emails on hand and quickly find them (for example court cases).

❯ Some states might require archiving (e.g. Germany: Very strict rules).

❯ Lightening the load on your email server.

Those are valid reasons to look for email archiving software - but there is more.

Email Archiving Solutions

There is an Archive on my Exchange Server. Isn't That Enough?

The simple answer is: Yes - and no. Depending on your expectations, the archive might suffice.

The longer answer is: It is not the optimal solution. An Exchange Server archive will simply collect every mail your business receives and sends. This means that every spam message, every phishing email, and every attachment (even those containing malware) will find its way into your archive.

A Question of Security

Outlook or the archive on your Exchange Server will store your emails but, they will not keep track of them. People with knowledge and access can manipulate emails without leaving a trace.

The offer you accepted read 1,000 USD when it arrived? Maybe, but after a little tampering with the email you kept in your "offers" folder suddenly reads 10,000 USD – just like the invoice in your inbox....

Professional Solutions Offer More

A professional email archiving solution (such as the Exchange Server Toolbox) will not only keep your emails in a safe place and protect your business. The Exchange Server Toolbox works on Exchange Server and hMailServer and comes with many additional features.

Spam Filter and Virus Protection

The Exchange Server Toolbox comes with the preconfigured spam filter SpamAssassin and the open source antivirus software ClamAV. Both work inside the Exchange Server Toolbox and will scan each email before delivering it to your inbox.

SpamAssassin is a great spam filter and it will continue to improve: Train spam and ham emails and tell your spam filter what to watch out for.

On Exchange Server 2001 and higher, emails with malware attachments or spam emails can be returned to the sender: Legally, they won't have been delivered, this might mean that you don't have to archive them.

Secure Email Archive and Archive Search

The Exchange Server Toolbox uses signatures to prevent unnoticed alterations to emails stored in the archive. For each archived email, a signature is created. The encrypted signature is comprised of a salted hash value created from the email and a timestamp.

What does that mean? In the example mentioned above you could easily prove that the email on your server is not the one you received and send.

Archiving software should enable your employees to find each and every archived email in a manner of seconds. The Exchange Server Toolbox comes with an archive search helping you find specific emails fast.

A customer has a question regarding an old order? Simply call up the email and help her out.

The best thing: Each user only sees the emails they are supposed to see.

Ease of Use: Outlook Add-in

The Exchange Server Toolbox offers an Outlook add-in enabling users to train spam emails and access the email archive search.

The Exchange Server Toolbox combines powerful protection with a secure email archive and easy user access. In short: It's your optimal email archiving solution.

The add-in is provided as an MSI file for easy deployment in professional environments.

Email Archiving Solutions

Best Practice: JAM Software

As a Germany-based company, JAM Software is subject to very strict archiving laws (the GoBD). Like any other business publishing contact details on the internet, JAM Software receives a huge amount of spam emails as well as emails containing viruses and malware.

The Exchange Server Toolbox keeps the inboxes safe and the servers lean.

Stop Spam: SpamAssassin

Spam emails are technically business offers and as such would have to be archived along with any other business correspondence according to the GoBD.

The spam filter SpamAssassin checks emails and assigns a spam score to each email. The Exchange Server Toolbox rule system processes the emails according to the spam score. At JAM Software the rules are:

> ❯ Spam score 0–3.4: Deliver the email to the inbox.
> ❯ Spam score 3.4–4.9: Deliver the email, but tag it as possible spam, the user decides.
> ❯ Spam score 5+: Return the email to sender.

When tagging a suspicious email, the Exchange Server Toolbox will add [spam] to a the email's subject and show the spam score.

Jane

[SPAM - Score: 3.8] Re: Plastic mould manufactuer
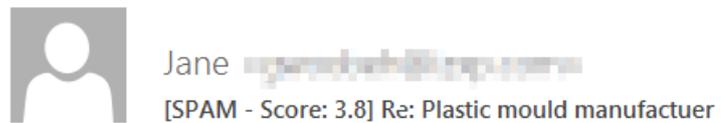
A tagged email showing the spam warning and the spam score of 3.8.

The user will use the Outlook Add-in to either tag the email as spam or as ham (thus training the SpamAssassin).

Malware Protection: ClamAV

If an email attachment contains malware, JAM Software's Exchange Server Toolbox will return the email to its sender. This ensures that no attachment is opened inadvertently and keeps the email archive free of malicious software.

The Exchange Server Toolbox offers an alternative solution to the malware problem. It can tag emails containing viruses and move any attached files to quarantine. The administrator receives an email containing the virus warning and a link to the file, the recipient is informed that a malicious attachment was removed from the email and is advised to contact the administrator.

Rule System: Intelligent Email Processing

When using the Exchange Server Toolbox, administrators can define their own rules regarding the processing of emails.

JAM Software has to archive all emails classified as business correspondence. Certain email types, however, are exempt from the GoBD obligations. The following emails are excluded from the archive:

> ❯ all emails tagged as "private"
> ❯ all emails created by software (e. g. the versioning and revision control system, the servers etc.)

The Exchange Server Toolbox recognizes the emails and keeps them from the archive.

Companies not subjected to strict archiving regulations can, for example, limit the timespan an email is kept in backup or only archive orders and offers. The Exchange Server Toolbox rule system is highly flexible and offers a wide variety of options.