The concentration of cloud (unfortunately) continues
Egg, November 24, 2023: *Open protocols are essential for the exchange of information in a networked world. Without the internet, the way we communicate with each other today would not exist. The standard protocols of the web guarantee that we have the choice, both now and in the future, that an exchange is possible and with which apps this should take place. However, the standard-compliant protocols of the internet are more tolerated than desired by tech companies. A current example is the new Outlook app under Windows.*

Outlook with IMAP now only via Microsoft Cloud
Until now, it was possible to set up Outlook with any mail provider. Now this is no longer possible. If the new Outlook app is activated under Windows, the password data (including passwords) is always saved in the Microsoft cloud when the mail service provider that receives the emails for customers and forwards them to the Outlook app (email client) is integrated. Microsoft then requests and processes all emails from the external email provider in its own cloud.
This destroys the basic idea of the web that information is exchanged in a standard-compliant manner. Microsoft can do with the accounts as it pleases. And this does not even refer to the scenario where Outlook itself is a little too curious, but to the fact that any third-party Microsoft applications can access these emails at any time and that these cloud services can change content without the end user being able to detect this at all (e.g. through increased activity on their own computer). More information on this topic can be found at **heise.de.**

The consequences are not entirely incidental

Of course, many will now object that it’s all half as bad. After all, nobody has to use Microsoft products, and certainly not Outlook. But the fact is that Outlook products are so well integrated into Microsoft’s Office apps and Teams that most companies ultimately rely on Outlook for this very reason. In the past, Outlook was an email client that could be used with any IMAP mail provider.
This is no longer the case. Anyone using the Outlook app can only use an alternative IMAP provider if Microsoft can read and write along without being asked and, moreover, always stores this data in the Microsoft cloud. In other words, anyone who uses the new Outlook app always agrees to all data being stored by Microsoft.

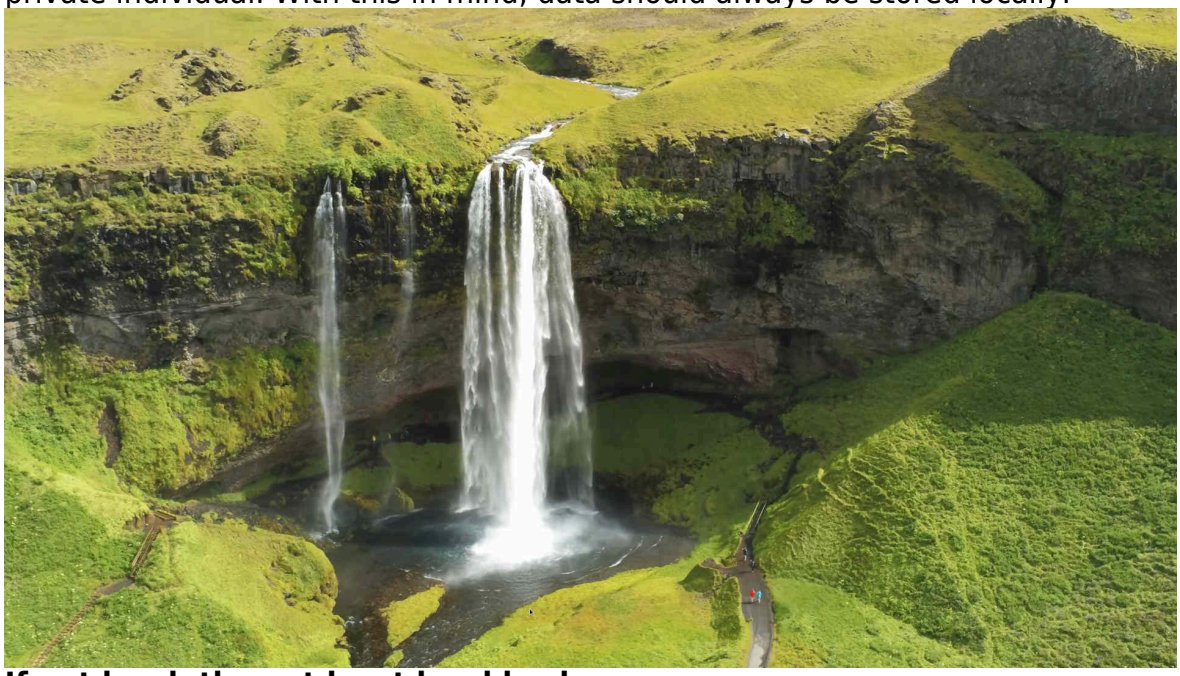
Does encrypting emails help?

Mails are currently encrypted using the S/MIME standard, for example. There is a private and a public key. The private key remains with the sender, the recipient receives the public key and can use it to read the encrypted message.

As long as the private key never leaves the sender's premises and the public key only remains with the recipient, encrypted emails offer quite good protection against unauthorized "reading" of the data. However, the private key must be stored in the mail client. How can it be ensured that these keys are not forwarded to Microsoft?
With closed source software (the source code is not disclosed), it is not possible to say what a program does or does not do. However, it is possible to determine whether or not information is being exchanged by recording the data traffic (logging). As long as Outlook therefore only sends data to the mail provider, it can at least be stated that this information is not sent to Microsoft.
With the new explicit "request" of the Outlook app to have access to all mail data of IMAP accounts not hosted by Microsoft, it is no longer possible to check which data is sent to Microsoft and which is not, including the keys. Encrypting emails therefore makes no sense, Microsoft can read them. Can does not mean that it will happen. But can means it is possible, and it should not.

Stalling the IMAP protocol
The IMAP protocol with SSL/TSL connection (port 993) offers standard-compliant mail communication from and to the mail provider. About a year ago, Office365 "blocked" access for third parties. As a result, mails could no longer be archived with the ArchivistaBox mail module. As a result, the Office 365 module was created this spring. This allows our customers to continue archiving their emails.
A small side note at this point: *Most of the emails were already archived in the ArchivistaBox. The ArchivistaBox mail module deleted the mails after processing them in the corresponding IMAP account. When the Office365 module was introduced, it came as a surprise that these mails were obviously only deleted (marked) in the IMAP view. Office365 spit out the mails again years later. So much for the confidentiality of Microsoft deleting emails.*
In addition to the IMAP transport protocol, there are now rules for the mail structure, i.e. the content of the mail is defined. This ensures that the mail can be read by the recipient. A sent mail should not be touched once it has reached the recipient (mail provider), as the job (sending a mail from X to Y) is complete. However, Office365 delivers mail messages according to its own criteria, i.e. once a mail has been retrieved, it is not delivered immediately when it is called up later. Although the differences are not massive, different IMAP contents of the same mail mean that no one can determine the uniqueness of a mail.

Tech companies are not interested in standards
Why is Microsoft doing this? As mentioned at the beginning, the big tech players are not interested in standard protocols being used. Because if this were the case, the programs could be replaced at will. If, on the other hand, more or less “closed” protocols are used, it is much easier to “bind” customers to a product, as there is quite a lot of migration pressure to overcome before a change can take place.
Here, too, a brief reference to the changeover of mail archiving from IMAP to Office365 in customer projects. With the IMAP protocol, dozens of mails could be processed per second; with the new Office365 protocol, Office365 spits out approx. 1 to 2 mails per second. In addition, the Microsoft cloud completely refuses to work for a few days after approx. 25,000 emails in a day. Therefore (and this does not only apply to Microsoft), once the data is in the cloud, it may only be possible to retrieve the data from the cloud with a great deal of effort (if at all!).
Data sovereignty only with local storage
The recent “behavior” of the Outlook app should also be understood in this context. It’s not about standards, but about power and, in this case, customer data. However, the scope can be extended, it’s not about whether the cloud is more secure or easier, it’s about the sovereignty of the data.
In terms of security, it is worth noting that the entire Microsoft cloud (all services) was fully compromised this summer, see, for example, the **ARD Tagesschau of September 8, 2023 (German).** Here, too, the horizon can be broadened, how many reports have there been this year that sensitive data of the Swiss Confederation has been hacked? Representative of many, the **BAZOnline with a recent report from today.**
Apart from the fact that sensitive data should never, ever end up on the darknet, data sovereignty is an even more important element. Being able to dispose of one’s own data is of central importance for every company and private individual. With this in mind, data should always be stored locally.



If not local, then at least local backup
If the central maintenance of programs and data appears to be too great an obstacle, you should at least make sure that the data is always stored locally and in a format that can be exchanged. In the case of e-mails, for example, this is the IMAP format. Even with our Office archiving, the mails are ultimately saved in IMAP format. The corresponding emails can also be reactivated in this

way.
Companies and private individuals who do not at least store data locally run the risk of suddenly being hit with a considerable amount of trouble. Have you ever thought about what happens if a Microsoft account is closed? Here, too, is a reference to an article on **PCSpezialist.de,** which reports on why this can happen and what consequences can be expected.
Ultimately, the new Outlook app for Windows is probably about Microsoft wanting to evaluate all emails in the cloud using “artificial intelligence” (AI). The benefits of these technologies are modest at best, but the collateral damage is likely to be considerable. For all these reasons, the Outlook app with cloud compulsion cannot be recommended for IMAP accounts. However, customers who use Microsoft’s Office Cloud will of course receive support for the Office365 module so that they can securely store their emails locally.