Wants a Global Backup Cooperation After Exchange Hack: "We could call it World Data Organization."

Interview: Companies have a tendency to forget their responsibility for their data in the cloud, shares Frederick Schouboe from the backup company Keepit. The Hafnium attack, which has compromised thousands of Exchange servers, emphasizes the need for having international cooperation on backup security measures.

Ditte Vinterberg Weng

"It would be great to have a global focus toward cooperating on security, especially in light of the Hafnium attack, which began to draw attention in early March." This is the opinion of Frederik Schouboe, Co-founder of Keepit, a company that sells backup solutions.

"A lot of Danish central authorities run communication and data storage on solutions such as Microsoft Office 365. If, for instance, the Microsoft Office 365 service was attacked by foreign powers, Denmark would stop functioning. This would be like the Mærsk hack, but on a national scale," he explains.

Even though Schouboe considered the scenario unlikely when Computerworld first spoke with him in the beginning of February, those following the infamous Hafnium attack during the past month might feel this comparison touches on something.

"Hafnium is an example of what is possible in the cloud, except things can be on a much greater scale," says Schouboe today.

"Therefore, as companies and as nations, we must be incredibly determined that this looming situation is changed.

A crash of an Exchange server can be devastating for an individual company," he explains.

"But if you roll it out on a large scale - as the Hafnium attack has shown is possible - then the consequence of the compromised systems can be overwhelming.

When the Exchange server provides services not just a single company, but an entire nation or continent, you can understand the powers at play when the server goes down," says Schouboe.

Moving to the cloud can be done without problems, the backup expert believes.

However, there is an issue that many people overlook when moving company data: There are no backup solutions for the individual user in most cloud-based services.

And this can cause problems with the GDPR.

Most people know the controversial EU directive as the set of rules that, in 2018, gave us the "right to be forgotten."

However, Article 32 of the GDPR states that the data controller – i.e., the company - must carry out "appropriate technical and organizational measures" to ensure the individual's data security: e.g., when a company collects personal data.

One of the ways to do this is by establishing the "ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident."

In one word: Backup.

The big danger, says Schouboe, is that many companies forget this responsibility when they move to the cloud - it may be on communication platforms such as Teams or Office 365, which do not provide backup for the individual user who uploads things.

The problem of companies not being aware of this lack of backup is divided into two problems.

Mistakes Can Be Costly

The first is the simplest to understand for most companies: it can result in a GDPR fine.

If a company or public authority ends up in the situation that they must be able to present data - for example in connection with a lawsuit - then the GDPR prescribes that the company must be able to "restore the availability of and access to personal data."

"In a lawsuit, for example, it may be necessary to recover an invoice with the individual's name on it, even if all the individual's information has been deleted," Schouboe explains.

"So, there are some situations where a document has the right to be forgotten. And if that document is in Teams or SharePoint, then the company itself has to ensure this."

This exact scenario played out in the Danish Health and Medicines Authority in January of last year, when crucial emails were deleted without the possibility of being recreated.

"These platforms that have emerged have a completely different approach to data protection. Not because they take it lightly, but because they can only manage their end of things. That's all they can do."

It is therefore the individual data processor's own responsibility to back up everything that is placed in cloud-based platforms.

"World Data Organization"

The second problem is, as mentioned, that the missing data can put an end to business operations in the event that the company, authority, or organization is hacked.

“Companies will have to assess their overall risk. For example, Microsoft 365 is now a far more interesting target for malicious hackers, and often a direct route into companies, and therefore it places even greater demands on suppliers and customers.”

In fact, the Keepit co-founder is convinced that the awareness of backing up data is a global problem if even leading players are not backing up. Therefore, it should also be a matter for national agencies, he believes.

"This is what I envision is necessary: to establish a worldwide technological and database agency - we could call it the World Data Organization (WDO)," declares Schouboe.

Schouboe sees the pandemic as proof that global cooperation towards a common goal is realistic when looking at how countries have cooperated during the crisis. And the ambitions are not over for the project.

"Nationally, at the same time, we should establish a data ministry which takes care of the national interests for IT and data security, but also makes investments and research in the field, so that we as a society are equipped for a more complex future without risking ending up as a country as Maersk did in connection with the NotPataya attack."

Not surprisingly, Frederik Schouboe also believes that it should be mandatory for companies to have a backup, "just as it is mandatory to have liability insurance when driving a car."