Security flaws in Microsoft email software raise questions over Australia's cybersecurity approach

Carsten Rudolph, Monash University

On March 2, 2021, Microsoft published information about four critical vulnerabilities in its widely used Exchange email server software that are being actively exploited. It also released security updates for all versions of Exchange back to 2010.

Microsoft has told cybersecurity expert Brian Krebs it was notified of the vulnerabilities in "early January". The Australian Cyber Security Centre has also issued a notice on the vulnerabilities.

The situation has been widely reported in the general media as well as specialist cybersecurity sites, but often inaccurately. But the situation also highlights a contradiction in government cybersecurity policy.

When governments find flaws in widely used software, they may not publish the details in order to build up their own offensive cybersecurity capabilities, i.e. the ability to target computers and networks for spying, manipulation and disruption. Operations like this often rely on exploiting vulnerabilities in commercial software — thus leaving their own citizens vulnerable to attack as a consequence.

What happened?

Microsoft has issued patches to fix the vulnerabilities and provided advice on how to respond if systems have already been affected.

These vulnerabilities can be really damaging for anybody running their own Exchange mail server. Attackers can run any code on the server and fully compromise a business's email, allowing them to impersonate anybody in the business. They could also read all email stored on the server and potentially compromise more systems within the businesses' network.

Who was affected?

It's important to clear up exactly who the vulnerabilities affected: anybody running their own instance of Exchange, and the risk was higher if web access was turned on.

An ABC/Reuters report said:

> All of those affected appear to run Web versions of email client Outlook and host them on their own machines, instead of relying on cloud providers.

But using a cloud-hosted version of Exchange wouldn't necessarily solve the problem, as the vulnerabilities still exist. What's more, larger enterprises will most probably still choose or be required by regulation to also run a local Exchange server that can be exploited in the same way.

Another open issue with moving mail servers to the cloud is that it also gives the provider access to all unencrypted emails by default. End-to-end encryption would increase security, but this is not currently standard practice.

Questions for Microsoft

As vulnerabilities existed in versions of the software released as long ago as 2010, we can assume more skilled attackers have already used them. This raises a fundamental question about the quality of the software, which Microsoft has been developing since 1996. Why did Microsoft not spot these vulnerabilities earlier?

Another question: if Microsoft knew about the vulnerabilities in early January, why did it take two months to alert its customers?

Questions for cybersecurity policy

We also need to consider the bigger picture of how we deal with vulnerabilities in software that builds the backbone of our computer and network infrastructure. Obviously, these vulnerabilities would have been a great offensive cybersecurity tool for any number of actors.

There is a basic conflict between building offensive cybersecurity capabilities and protecting our own businesses and citizens.

Imagine you are tasked with building offensive cybersecurity capabilities. You discover these vulnerabilities in Microsoft Exchange. Would you alert the vendor, Microsoft in this case, to make sure they are fixed as soon as possible, or would you keep them secret to not to lose your great new cyber weapon? Secretly having access to an organisation's email could be very valuable for law enforcement or intelligence agencies.

Australia's Cyber Security Strategy 2020 does not address the contradiction between establishing offensive cybersecurity capabilities and protecting Australians from cybersecurity vulnerabilities.

The establishment of offensive cybersecurity capabilities is explicitly mentioned in the strategy. In contrast, the detection of vulnerabilities with the goal of mitigation is not a clear goal.

Nor is openness about existing vulnerabilities — which would empower Australian citizens to react to them — part of the strategy. Australia has the expertise across the public sector, private sector and civil society to have this important dialogue on how to best protect Australian citizens and businesses.

Carsten Rudolph, Associate professor, *Monash University*