Article

Dec 2021

Is on-premise Exchange Server dead?

Over the past couple of months I have supported too many organisations with rebuilding an Exchange Server environment that has been compromised due to an unpatched vulnerability. Which has left me questioning, how viable is an on-premise Exchange Server in today's cloud-focused IT landscape?

Vincent Sharp
Executive Technology Consultant
Email vincent.sharp@waterstons.com

Exchange Online is undeniably increasing in popularity, with more organisations adopting it over on-premise Exchange Server and other solutions for a variety of reasons; some are keen on better integration with other Microsoft 365 services, others like having the latest features, and the reduction in maintenance time and cost is attractive to many. That said, in my opinion, a well designed and managed on-premise Exchange Server environment will continue to be more stable than Exchange Online, suffering less service degradation or issues. To achieve this stability, the solution needs to be designed to be resilient, have good backups, and have the right level of monitoring in place to detect and respond to problems, ideally before they occur. Crucially, IT support teams need to have the right level of expertise and resources to manage and maintain the solution.

The past year has not been kind to Exchange Server, with some severe vulnerabilities discovered and requiring urgent patches in March, July, October and November. One of the more interesting features released recently in Exchange was the Emergency Mitigation service, where by default Exchange servers check hourly to see if Microsoft have released any new mitigations for known vulnerabilities, and apply these automatically. This is unlikely to be perfect, and will not protect against unknown vulnerabilities, or those that cannot be protected against through URL pattern-matching.

All that said, there is still a use case for on-premise Exchange Server for enterprises for whom email is a business-critical function, where stability is more important than the newest features and other benefits that Exchange Online can provide.

What can be done to better protect Exchange Server?

First and foremost, keep on top of your patching! It is essential that your IT teams are able to apply critical updates to Exchange services quickly. In a highly available solution this can generally be done with minimal to no disruption; for solutions without application-level redundancy the business will need to balance the risk of not patching quickly enough with the impact of the maintenance window.

Microsoft have also published and regularly update an Exchange Server Health Check script, which checks your server against various known vulnerabilities and best practice recommendations to keep your server as secure and performant as possible. Consider running this against your environment regularly and adopt the recommendations it gives you.

Secondly, make sure that Exchange Server is not directly published to the internet. At minimum, a reverse proxy solution should reside on a DMZ network to pass internet requests to your Exchange service, improving security by obscuring internal server information, and better ensuring that only requests for legitimate content and addresses are served. Some reverse proxies can also provide safeguarding against network-based attacks like Denial-of-Service.

Even better, a Web Application Firewall (WAF) is a more advanced form of reverse proxy that more intelligently responds to requests and their behaviour and is often capable of blocking activity based on how suspicious it looks. If you are already using WAFs it is likely you were protected against some of the recent Exchange vulnerabilities, even if you hadn't yet patched your services. A properly configured WAF is the best defence against unknown vulnerabilities in Exchange server, and any other web applications.

Whilst on the subject of external publishing, lets also talk MFA. You should be securing any internet-facing services with some form of Multi-Factor Authentication, whether that be a cloud service, a VPN or a web application like Exchange Server. This provides protection for your end-user accounts in the unfortunate, but these days almost inevitable, event of a credential leak. Options for Exchange include an MFA solution tied into your WAF or reverse proxy, or by making use of Hybrid Modern Authentication.

Next, be sure to have a robust message hygiene solution in place, and OS-level endpoint protection installed on each server (with appropriate exclusions of course). My own preference is to make use of a cloud-based message hygiene solution for both inbound and outbound emails, so the processing effort and suspicious emails can stay away from your live email servers. EDR (Endpoint Detection and Response) and SIEM (Security Information and Event Management) solutions can further improve your ability to quickly detect and respond to potential threats.

If the worst does happen, it's essential for you to have regular application-aware backups of your email environment. These should be tested regularly through a restore rehearsal, with a copy stored offline (or otherwise immutable from change) so it cannot be destroyed by a malicious attack.

If you have migrated to Exchange Online and have directory synchronisation in place, it's likely you'll have kept an on-premise Exchange Server for ongoing management, and to stay in a supported state. If you have an Exchange hybrid but no longer have any mailboxes on premises, you can probably reduce your attack surface by retiring the hybrid and unpublishing Exchange from the internet. The regular patching and backup advice still applies, but you need to be on the latest or previous Cumulative Update of Exchange Server to stay in support anyway.

In summary, if you intend to maintain an on-premise Exchange Server solution, then patch regularly, maintain good backups, take advantage of the Exchange Server Health Check script, and consider use of a Web Application Firewall to add an extra layer of protection against vulnerabilities. If this all sounds too complex, too expensive or too much effort to maintain, you should seriously consider migrating your email services to Exchange Online and let Microsoft manage your maintenance and Web Application Firewalling for you.

If you'd like help with either migrating to Exchange Online or improving the security of your Exchange Server solution, get in touch with one of our Technology Consultants by calling us on 0345 094 0945, or click here for more information on our team.