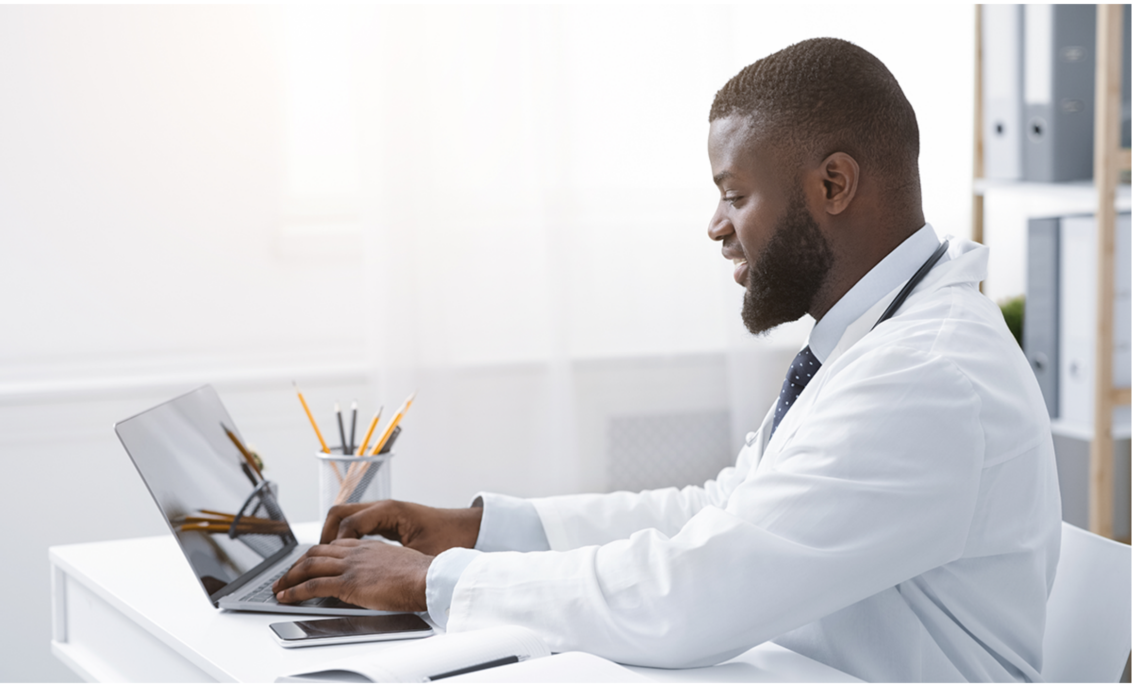
Microsoft Vulnerability Highlights Steps We All Need to Take



By Brian Johnson

A recently discovered vulnerability[1] in Microsoft's popular Exchange email server puts companies using this application at extreme risk. Security researchers have dubbed this event Hafnium, named after the Chinese-based espionage group first seen attacking servers. Once compromised, multiple backdoors[2] are installed on systems that will likely lead to complete takeover of hacked systems. As of March 5th, over 30,000 U.S.-based companies were known to be compromised. If you are running a Microsoft Exchange server[3], hopefully you have addressed this issue; if not, you need to act now and install emergency patches[4] provided by Microsoft. Security researchers at UNIT221B have put together several resources that include links to patches, methods to test your server, and resources to restore a compromised server. Investigative reporter, Brian Krebs, has a detailed article on the issue at KrebsonSecurity.com.

Major security events such as this are a reminder to evaluate your own security practices and prepare for the next big event. This incident demonstrates how fast cybercriminal groups will pounce on the opportunity to exploit vulnerable systems, so it is a good time to highlight security practices that can help defend against future threats.

The Hafnium incident demonstrates the classic cat-and-mouse game between cybercriminals and software vendors. Cybercriminals discover a vulnerability that can be exploited, and the software vendor releases a security patch to fix the issue. Unfortunately, releasing a patch broadly publicizes the existence of the vulnerability. Cybercriminals then race to exploit the weakness before the patch is fully deployed[5]. As a result, this leaves a small window for organizations to patch systems before cybercriminals can attack. Companies that develop routine procedures to patch and update systems will fare better in these situations. **It is important to know your systems and applications and how each is updated.** Microsoft, for example, releases patches for Windows and Office the second Tuesday of every month, a day known as “Patch Tuesday.” This process can be automated, ensuring that systems are fully patched and protected. Some applications, such as Chrome and Edge browsers, can also be configured to auto update. Other applications may require a manual download and install of the patch, as was the case to patch Exchange servers against Hafnium. Now is the time to inventory your systems and applications, learn how they are patched, automate where possible, and implement routine procedures.

Backups[6] are a safety net that can help save the day and restore a compromised system back to normal operation after a security event. Consider a ransomware[7] scenario where cybercriminals encrypt and hold your data captive until a monetary payment, usually in Bitcoin[8], is made. A good backup allows you to forego the ransom payment and restore your systems back to normal. Like the patching process, every software application has a different backup method. **It is important to understand your application, what data you are backing up, and how to restore it.**   Additionally, test your backups periodically to ensure that you are correctly saving the data and it can be restored to a usable state. Store your backups in a safe place, preferably on removable media or in the cloud away from your network. If cybercriminals can compromise your network and install ransomware, they will have enough access to find and destroy your backups, increasing the odds that you will pay the ransom.

A good security strategy includes an incident response plan. At a minimum, **know who you are going to call after a security event.** You will need a skilled security expert to perform a forensic investigation[9], clean your systems, and ensure the holes are plugged. If your incident involves the disclosure of protected information such as health or financial records, you will be required to notify the victims and the government and possibly provide identity and credit monitoring services.

If you encounter a security incident, contact SVMIC immediately to start the mitigation process. Your cyber liability insurance policy will provide the necessary resources and cover the cost of recovery within the limits of your policy. Additionally, SVMIC members can access much more information regarding cyber risk assessment and prevention at vantage.svmic.com.

[1] Hole or a weakness in the application, which can be a design flaw or an implementation bug, that allows an attacker to cause harm to the stakeholders of an application

[2] Feature or defect of a computer system that allows surreptitious unauthorized access to data

[3] Mail *server* and calendaring *server* developed by *Microsoft*.

[4] Set of changes to a computer program or its supporting data designed to update, fix, or improve it.

[5] Software tool designed to take advantage of a flaw in a computer system, typically for malicious purposes such as installing malware.

[6] Copy of computer data taken and stored elsewhere so that it may be used to restore the original after a data loss event.

[7] Type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

[8] Cryptocurrency invented in 2008 which began use in 2009; currently (March 2021), 1 Bitcoin = approximately $57,300 USD.

[9] Gathering and analysis of all related physical evidence in order to come to a conclusion.

The contents of The Sentinel are intended for educational/informational purposes only and do not constitute legal advice. Policyholders are urged to consult with their personal attorney for legal advice, as specific legal requirements may vary from state to state and/or change over time.