INSURANCE OFFICE OF AMERICA

Cyber Market Update

The recent Microsoft Exchange Server hack demonstrates the need for cyber liability insurance, but securing coverage may prove challenging amid a hardening market.

On March 2, 2021, Microsoft announced the detection of four flaws in on-premise Exchange Server versions 2013 through 2019. The weaknesses were exploited in a complex attack from a Chinese-based espionage group dubbed "Hafnium," which primarily targets United States businesses for the purpose of exfiltrating information.

In response, Microsoft quickly released security updates and encouraged prompt application of the patches as the best protection against the attack. Government organizations followed suit with the Department of Homeland Security and the Cybersecurity & Infrastructure Security Agency (CISA) ordering the immediate application of the updates. The Federal Bureau of Investigations (FBI) elected to take things a step further. "In a somewhat unprecedented move, the FBI forcibly removed exploited Exchange servers to prevent further impact," said GreyCastle, a leading cybersecurity services provider.

Hafnium, which conducts its operations from leased virtual private servers in the U.S., may have started the attacks, but other advanced persistent threat (APT) groups quickly followed, exacerbating the vulnerability on a global scale. Microsoft has continued its response, including the release of a one-click mitigation tool on March 15. By March 22, it claimed 92% of servers were either patched or mitigation had been applied. However, the full damage is yet unknown.

With an estimated number of companies affected as high as 30,000 in the U.S. and 250,000 globally, it is clear the hack presents a serious threat. The first recommendation for businesses using the software is to apply patches immediately. Some recommend moving to Microsoft 365 to avoid the issues faced by Exchange Server users. In addition to systems-related responses, other risk mitigation such as cyber liability insurance should be considered.

INSURANCE CARRIER RESPONSE

Since the attack, insurance carriers have employed various approaches in dealing with the increased risks identified by the Microsoft Exchange Server vulnerabilities. Some carriers have put a moratorium on new business for any accounts with on-premises Exchange Servers. So far, these have been open ended with no date given for when the moratorium will be lifted.

Carriers also have responded by requiring new supplemental applications to determine the likelihood of a compromise. In the case of the recent hack, specific details regarding actions taken by a business may need to be provided before terms are offered. Some carriers also are conducting systems analyses so clients can correct vulnerabilities or add additional security, such as multifactor authentication, before offering a quote for coverage.

CYBER LIABILITY COVERAGE

Those businesses that have a good cyber liability policy should be fully covered for anything relating to the Exchange Server vulnerability, providing that the resulting loss was insured against, the vulnerability was only a means of the hackers entering the system, and the type of loss would be determined by what the hacker does once the system is infiltrated. For example, a hacker might install ransomware and lock down a network, extract private Information, or view bank account information and attempt to access the company's funds directly.

> The massive web of malicious software that is spread by these attacks can take months to sort out, and the losses to businesses can cost millions of dollars to rectify.

Hackers will monitor emails for months, adding rules so that they can send and receive emails on the businesses behalf without it knowing. They watch the flow of client relationships, billing, and financial transactions. Their hope is to use your network as a long-term attack vector to trick your clients into wiring funds to them or to spread malware for them. Hackers can use your email to spread ransomware to other entities, causing hundreds

DISCLAIMER: The information contained here is intended to be general and advisory in nature. It is not to be considered legal advice of any kind.

of thousands or even millions of dollars in losses. The massive web of malicious software that is spread by these attacks can take months to sort out, and the losses to businesses can cost millions of dollars to rectify.

There is some good news, however. “We observed in response to this latest threat that, although a lot of people were impacted, it has been minimal so far and did not involve manual interaction with or exfiltration from the asset,” said GreyCastle.

SECURING COVERAGE BEFORE IT’S TOO LATE

The bottom line is, if you use Microsoft Exchange Server and you do not yet have cyber insurance, the hurdle is going to be higher today than before for purchasing coverage. We are in the midst of a significant hardening of the cyber insurance market. Many renewals are coming in at 30% to 100% higher than the previous year, and there are many customers who are not being renewed and for which no replacement coverage offerings are available.

Getting coverage in place now is going to be the most prudent course of action for any business. Should there be another similar event where the insurance market takes such a dramatic approach to the risks faced by businesses, it will be advantageous to have coverage in place beforehand. Similar to the inability to insure a property once it is in the path of a named storm or a building in the path of an impending wildfire, carriers are not going to offer coverage if a client has a significant known security vulnerability.

For more information surrounding this vulnerability, including scripts that can be executed, indicators of compromise (IOC), and context, see the below resources.

- Microsoft’s Advisory and Security Blog Post
- Microsoft’s Patch Release
- CISA Alert (AA21-062A)

Contact your IOA insurance advisor today to discuss your risk management needs and how you can be protected against cyberthreats.

DISCLAIMER: The information contained here is intended to be general and advisory in nature. It is not to be considered legal advice of any kind.