KRIEG DEVAULT

Insights

Constant Vigilance! Recent Microsoft Exchange Hack Reveals the High Cost of Letting Your Guard Down.

April 20, 2021

By: Brandon W. Shirley and Shelley M. Jackson

In March 2021 the Microsoft threat center **announced** a significant cyberattack that affected certain Microsoft Exchange users with on-premises servers throughout the world. For at least two months, hackers apparently successfully exploited vulnerabilities in the Microsoft Exchange system, giving them substantial access to certain entities' networks. Health care providers should be particularly concerned with this attack given their increased use of electronic platforms to conduct business, see patients, and to maintain health records. Microsoft has since released security patches to close the gaps, and companies using Microsoft Exchange **are urged** to immediately install them. Microsoft continues to provide periodic updates, with **the latest** on March 25, 2021 detailing the three prevailing threat trends: **web shells**, **human-operated ransomware**, and **credential theft**.

As health care providers continue to be among the top targets for data breaches, such entities should take each threat seriously (even if they were not an affected target in this particular cyberattack) and take immediate steps to address the issues and guard against future attacks. Notably, the Health and Human Services Office of the Assistant Secretary for Preparedness and Response recently **highlighted** that health care providers represented 41% of all cyberattacks in 2020. The threat to health care providers will likely increase as providers continue to use technology platforms to conduct telehealth visits, maintain patient records, and grapple with **ONC's information blocking and interoperability rules**.

Health care providers' legal and financial costs of data breaches can be significant. The financial penalties vary depending on the circumstance and scope of the breach but can easily run into the **millions of dollars**. Health care providers may also face legal exposure when individuals affected by a breach sue the targeted health care provider. While the **legal theories** for these lawsuits may vary, they commonly allege negligence, e.g., maintaining data in a reckless manner or dangerous condition, failing to comply with minimum security standards, or failure to implement and follow basic security procedures. The widespread nature of the Microsoft breaches may also subject health care providers to class action lawsuits, which potentially compound a provider's financial exposure.

Health care providers can protect themselves from incurring such legal and financial costs through various means, including:

- Incorporating cybersecurity matters as a core part of an enterprise-wide risk management program, including purchasing comprehensive cyber insurance coverage and regularly updating coverage types and limits as appropriate.
- Implementing robust cybersecurity policies and procedures and updating them regularly based on the latest industry guidelines.
- Subscribing to Government or other agency **distribution lists** that provide updates and information about data threats or that provide helpful resources.
- Conducting employee training throughout the year with an emphasis on identifying and avoiding credential theft attempts, such as email phishing scams, and responding to attempted or successful ransomware attacks.
- Identifying persons responsible for immediately installing security patches when available, particularly when vulnerabilities like the Microsoft hack are disclosed.

If you need help with your company's cybersecurity policies or training, or if you have concerns regarding an authorized disclosure or potential data breach, contact **Brandon W. Shirley** or **Shelley M. Jackson**.

This article should not be construed as legal advice or legal opinion. The content is intended for general informational purposes only.