Scathing federal report rips Microsoft for shoddy security, insincerity in response to Chinese hack

April 3 2024, by Frank Bajak

The Microsoft logo is seen in Issy-les-Moulineaux, outside Paris, France, April 12, 2016. In a scathing indictment of Microsoft corporate security and transparency, a Biden administration-appointed review board issued a report

Tuesday, April 2, 2024, saying “a cascade of errors” by the tech giant let state-backed Chinese cyber operators break into email accounts of senior U.S. officials including Commerce Secretary Gina Raimondo. Credit: AP Photo/Michel Euler, File

In a scathing indictment of Microsoft corporate security and transparency, a Biden administration-appointed review board issued a report Tuesday saying "a cascade of errors" by the tech giant let state-backed Chinese cyber operators break into email accounts of senior U.S. officials including Commerce Secretary Gina Raimondo.

The Cyber Safety Review Board, created in 2021 by executive order, describes shoddy cybersecurity practices, a lax corporate culture and a lack of sincerity about the company's knowledge of the targeted breach, which affected multiple U.S. agencies that deal with China.

It concluded that "Microsoft's security culture was inadequate and requires an overhaul" given the company's ubiquity and critical role in the global technology ecosystem. Microsoft products "underpin essential services that support national security, the foundations of our economy, and public health and safety."

The panel said the intrusion, discovered in June by the State Department and dating to May "was preventable and should never have occurred," blaming its success on "a cascade of avoidable errors." What's more, the board said, Microsoft still doesn't know how the hackers got in.

The panel made sweeping recommendations, including urging Microsoft to put on hold adding features to its cloud computing environment until

"substantial security improvements have been made."

It said Microsoft's CEO and board should institute "rapid cultural change" including publicly sharing "a plan with specific timelines to make fundamental, security-focused reforms across the company and its full suite of products."

In a statement, Microsoft said it appreciated the board's investigation and would "continue to harden all our systems against attack and implement even more robust sensors and logs to help us detect and repel the cyber-armies of our adversaries."

Commerce Secretary Gina Raimondo, left, listens during a Senate Commerce, Science, and Transportation hearing titled "CHIPS and Science Implementation and Oversight", Wednesday, Oct. 4, 2023, on Capitol Hill in Washington. a

scathing indictment of Microsoft corporate security and transparency, a Biden administration-appointed review board issued a report Tuesday, April 2, 2024, saying “a cascade of errors” by the tech giant let state-backed Chinese cyber operators break into email accounts of senior U.S. officials including Commerce Secretary Gina Raimondo. Credit: AP Photo/Mariam Zuhaib, File

In all, the state-backed Chinese hackers broke into the Microsoft Exchange Online email of 22 organizations and more than 500 individuals around the world including the U.S. ambassador to China, Nicholas Burns—accessing some cloud-based email boxes for at least six weeks and downloading some 60,000 emails from the State Department alone, the 34-page report said. Three think tanks and foreign government entities, including a number of British organizations, were among those compromised, it said.

The board, convened by Homeland Security Secretary Alejandro Mayorkas in August, accused Microsoft of making inaccurate public statements about the incident—including issuing a statement saying it believed it had determined the likely root cause of the intrusion "when, in fact, it still has not." Microsoft did not update that misleading blog post, published in September, until mid-March after the board repeatedly asked if it planned to issue a correction, it said.

Separately, the board expressed concern about a separate hack disclosed by the Redmond, Washington, company in January—this one of email accounts including those of an undisclosed number of senior Microsoft executives and an undisclosed number of Microsoft customers and attributed to state-backed Russian hackers.

The board lamented "a corporate culture that deprioritized both enterprise security investments and rigorous risk management."

The Chinese hack was initially disclosed in July by Microsoft in a blog post and carried out by a group the company calls Storm-0558. That same group, the panel noted, has been engaged in similar intrusions—compromising cloud providers or stealing authentication keys so it can break into accounts—since at least 2009, targeting companies including Google, Yahoo, Adobe, Dow Chemical and Morgan Stanley.

Microsoft noted in its statement that the hackers involved are "well-resourced nation state threat actors who operate continuously and without meaningful deterrence."

The company said it recognizes that recent events "have demonstrated a need to adopt a new culture of engineering security in our own networks," adding it has "mobilized our engineering teams to identify and mitigate legacy infrastructure, improve processes, and enforce security benchmarks."