Microsoft faces heat from US Congress over cybersecurity

June 14 2024

Microsoft President Brad Smith spent more than three hours answering questions from members of the Homeland Security Committee in Washington.

Members of US Congress on Thursday pressed Microsoft to explain a "cascade of avoidable errors" that allowed a Chinese hacking group to

breach emails of senior US officials.

Microsoft President Brad Smith spent more than three hours answering questions from members of the House Committee on Homeland Security in Washington, assuring them cybersecurity is being woven more deeply into the technology company's culture.

"Microsoft accepts responsibility for each and every one of the issues cited" in a scathing US government report about the breach "without equivocation or hesitation," Smith told the committee.

The Cyber Safety Review Board (CSRB), led by the US Department of Homeland Security, conducted a seven-month investigation into the incident last year that involved the China-affiliated cyberespionage actor Storm-0558.

"Microsoft has an enormous footprint in both government and critical infrastructure networks," US congressman and committee member Bennie Thompson said to Smith as the hearing opened.

"It is our shared interest that the security issues raised by the (report) be addressed quickly."

The operation, which was first discovered by the US State Department in June 2023, included hacks on the official and personal mailboxes of Commerce Secretary Gina Raimondo and US Ambassador to China Nicholas Burns.

Microsoft's core business is to provide cloud computing services, such as Azure or Office360, that host sensitive data and power business and government operations across major sectors of the economy.

The report criticized a Microsoft corporate culture that was "at odds

with... the level of trust customers place in the company."

The review identified a series of operational and strategic decisions by Microsoft that opened the door to the breach, including the failure to identify a new employee's compromised laptop following a corporate acquisition in 2021.

It also found that Microsoft fell short of safety standards seen at competing cloud companies, including Google, Amazon and Oracle.

"The Board finds that this intrusion was preventable and should never have occurred," the review said, pinpointing "the cascade of Microsoft's avoidable errors that allowed this intrusion to succeed."

'Lasting change'

The report also recommended that Microsoft develop and publicly release a plan with timelines to enact wide-ranging security reforms across its products and practices.

"The real challenge is how you achieve effective lasting cultural change," Smith said, noting Microsoft has nearly 226,000 employees.

Smith said Microsoft has the equivalent of 34,000 engineers working full time on answering the security shortcomings in "the largest engineering project focused on cybersecurity in the history of digital technology."

Microsoft's board on Wednesday approved a change that will tie cybersecurity accomplishments with annual bonuses for senior executives and make it part of every employee's annual review, according to Smith.

Microsoft detects some 300 million cyberattacks on its customers daily, with most of those coming from China, Iran, Korea, Russia, or ransomware operations, Smith told the committee.

"We're dealing with four formidable foes in China, Russia, North Korea and Iran, and they are getting better," Smith said.

"We should expect them to work together; they're waging attacks at an extraordinary rate."

While it is inevitable that adversaries will use artificial intelligence for increasingly sophisticated attacks, the technology is already being used to strengthen cyber defenses, Smith added.

Citation: Microsoft faces heat from US Congress over cybersecurity (2024, June 14) retrieved 26 June 2024 from https://techxplore.com/news/2024-06-microsoft-congress-cybersecurity.html