12M Daily Slack Users Sharing Proprietary Company Info, What Could Go Wrong?

Posted by Karen Heumann, January 18, 2023

Slack is used by 100k+ organizations, including 77 of the Fortune 100 companies. Slack breaks down silos and creates an open forum for troubleshooting, sharing ideas, finding common interests, and venting. But, 12M+ daily users (and, a jaw-dropping 79M+ users expected by 2025) and rapid-fire exchange, across multiple channels, with people you have never met before, creates a cybersecurity risk rich environment. The benefit of Slack? Users relax and collaborate freely. The risk? Users don't consider the hacking risks and may not question whether the person asking for confidential data is the authorized recipient of that information or may click on a shared article without the poster or viewer recognizing the document is infected. Obviously, it is not the fault of the platform if someone mistakenly or maliciously shares an infected document, but the risks should be recognized and minimized. Just as employees are trained to recognize phishing emails, consideration should be given to the risks inherent in Slack, and other communication platforms.

End-to-end encryption is becoming a standard means to secure digital conversations, authorizing only the sender and the recipient to view the messages and all the data contained within. However, Slack does not have end-to-end encryption in order to retain visibility into communications across working groups and slack channels. Slack does use HTTPS encryption, DLP integrations, and its own Enterprise Key Management (EKM) for data protection. This means data is encrypted both enroute and while at rest on Slack's servers. If a hacker obtained the decryption key, they could access all the messages sent across the platform, including confidential data, and more importantly, the thought processes behind developing, resolving, and addressing product development, revenue strengths and weaknesses, planned projects, sales metrics, personnel grievances, and company strategy. The huge volume of message-creation on Slack provides an especially large attack surface.

Slack was hacked in December. The security team found that some Slack employee tokens were stolen and used to access the company's GitHub external repository. No downloaded repositories contained customer data. Also, last July an independent security researcher discovered a vulnerability

when the platform transmitted a hashed version of the user password to other workspace members. This hashed password was not visible to any Slack clients and discovering it required actively monitoring encrypted network traffic coming from Slack's servers. The flaw affected all users who created or revoked shared invitation links between April 2017 and July 2022.

BetterCloud's Christina Wang is concerned that Slack users with "Owner" and "Admin" roles have significant power, often more than most administrators realize. For example, Wang says, "By default, only Slack Workspace Admins and Owners can create and manage user groups. But any admin can change those settings in a drop-down menu." Effectively, any one of your organization's admins can go in and make it possible for all of a workspace's users to create, modify or disable user groups.

Ars Technica reported that "A surprisingly large number of developers are posting their Slack login credentials to GitHub and other public websites." Despite Slack declaring that access tokens should be treated with the same level of care as passwords. The Origin Report's Josh Fraser shared that the 1,118 members of its open Slack community had their personal information — including their email addresses, usernames, real names, profile pictures, last updated timestamps and timezone settings — exposed by a hacker who manipulated API keys.

Also, very little is known about which Slack team members can access user data, and when they can do it. Slack claims to have technical, audit and policy controls in place to prevent inappropriate access, they also acknowledge that they did not intentionally build an app that would prevent employees from accessing information without authorization. Electronic Frontiers Foundation Senior Staff Attorney Nate Cardozo says, "Slack could have built this system in a way that no one within the company had access into user data," referencing zero-knowledge encryption, an end-to-end encryption method. "What it comes down to is, trust us.'"