Mphasis
The Next Applied

6 Prompts You Don't Want Employees Putting in Microsoft Copilot

Date: 03rd April 2024 | Severity: High

Summary

Crowned the greatest productivity tool in the age of AI, Microsoft Copilot is a powerful asset for companies today.

But with great power comes great responsibility.

If your organization has low visibility of your data security posture, Copilot and other gen AI tools have the potential to leak sensitive information to employees they shouldn’t, or even worse, threat actors.

Attack Vectors

People have access to way too much data. The average employee can access 17 million files on their first day of work. When you can’t see and control who has access to sensitive data, one compromised user or malicious insider can inflict untold damage. Most of the permissions granted are also not used and considered high risk, meaning sensitive data is exposed to people who don't need it.

When sensitive information lives in places that it's not supposed to, it becomes easily accessible to everybody in the company and the gen AI tools they use.

Indicator of Compromise

Not Applicable

Recommendation

Before you enable Copilot, you need to properly secure and lock down your data. Even then, you still need to make sure that your blast radius doesn’t grow, and that data is used safely.

Reference Links

https://www.bleepingcomputer.com/news/security/6-prompts-you-dont-want-employees-putting-in-microsoft-copilot/

https://www.varonis.com/blog/6-prompts-you-dont-want-employees-putting-in-copilot-varonis?utm_campaign=Copilot%20Campaign&utm_source=Sponsored%20PR&utm_content=6%20Prompts%20Original%20Blog%20-%20Bleeping%20Computer