NEED TO KNOW NEWSLETTER | OCTOBER 2025

Ransomware rampage!

Lessons from Volvo's ransomware data breach

Car manufacturer Volvo North America has announced that it suffered a data breach in August 2025. Hackers used ransomware to target third-party provider Miljödata, which supplies IT resources for human services. Volvo North America was one of more than two dozen organizations affected by the Miljödata data breach.

This month, we're reviewing the lessons we can learn from this latest ransomware attack.

Hitting third-party services hurts multiple orgs at once

Miljödata's IT services were used by Volvo NA, an airline, a metals company, and even local government in Sweden. One attack compromised all of them. Hackers love big targets!

Attacks keep getting bigger

This attack compromised about 870,000 records, including Social Security numbers, home addresses, and even medical data. But that doesn't even put it in the top ten most destructive data breaches of the last few years. Today, millions of records are routinely exposed by cyberattacks.

Attackers won't always wait to be paid

The hackers demanded a ransom of 1.5 Bitcoin to release the stolen data. However, reports were already flying about potential data leaks. Miljödata refused to pay, and the stolen data was published ... but we don't know how soon the data reached the Dark Web. These days, hackers might not wait to share.

Staying safe from ransomware

Ransomware is just another type of malware, and that means the malware rules apply. Follow these tips to help keep your workplace ransomware-free!

- Don't click on unsolicited documents or downloads! Hackers can embed malware in files, even PDFs!
- Report any unusual system behavior or unusual pop-up messages
- Use a VPN when outside your secure system. Traveling? Working remotely? Keep that VPN on!
- Back up your backups! Ransomware only works when you don't have the data the attackers have locked.

The biggest ransomware attacks ... so far!

Chances are that you've been affected by a ransomware attack, even if you didn't know it. Major attacks include the Synovis/U.K. National Health Services attack (June 2024), which exposed the data of **almost 1 million people**; the Ascension attack (May 2024), which exposed the data of **5.6 million people**; and the Change Healthcare attack, which exposed the data of over **100 million people.**