

Car dealerships in North America revert to pens and paper after cyberattacks on software provider

June 24 2024, by Wyatt Grantham-Philips



Vehicles sit in a row outside a dealership, June 2, 2024, in Lone Tree, Colo. Car dealerships across North America have faced a major disruption this week. CDK Global, a company that provides software for thousands of auto dealers in the U.S. and Canada, was hit by back-to-back cyberattacks on Wednesday, June 19, 2024. Credit: AP Photo/David Zalubowski, File

Car dealerships in North America are still wrestling with major disruptions that started last week with cyberattacks on a company whose software is used widely in the auto retail sales sector.

CDK Global, a company that provides software for thousands of auto dealers in the U.S. and Canada, was hit by back-to-back cyberattacks Wednesday. That led to an outage that has continued to impact operations.

For prospective car buyers, that's meant delays at dealerships or vehicle orders written up by hand. There's no immediate end in sight, but CDK says it expects the restoration process to take "several days" to complete.

On Monday, Group 1 Automotive Inc., a \$4 billion automotive retailer, said it is using "alternative processes" to sell cars to its customers. Lithia Motors and AutoNation, two other dealership chains, also disclosed that they implemented workarounds to keep their operations going.

Here is what you need to know.

What is CDK Global?

CDK Global is a major player in the auto sales industry. The company, based just outside of Chicago in Hoffman Estates, Illinois, provides software technology to dealers that helps with day-to-day operations—like facilitating vehicle sales, financing, insurance and repairs.

CDK serves more than 15,000 retail locations across North America, according to the company.

What happened last week?

CDK experienced back-to-back cyberattacks on Wednesday. The company shut down all of its systems after the first attack out of an abundance of caution, according to spokesperson Lisa Finney, and then shut down most systems again following the second.

"We have begun the restoration process," Finney said in an update over the weekend—noting that the company had launched an investigation into the "cyber incident" with third-party experts and notified law enforcement.

"Based on the information we have at this time, we anticipate that the process will take several days to complete, and in the interim we are continuing to actively engage with our customers and provide them with alternate ways to conduct business," she added.

In messages to its customers, the company has also warned of "bad actors" posing as members or affiliates of CDK to try to obtain system access by contacting customers. It urged them to be cautious of any attempted phishing.

The incident bore all the hallmarks of a ransomware attack, in which targets are asked to pay a ransom to access encrypted files. But CDK declined to comment directly—neither confirming or denying if it had received a ransom demand.

"When you see an attack of this kind, it almost always ends up being a ransomware attack," Cliff Steinhauer, director of information security and engagement at the National Cybersecurity Alliance. "We see it time and time again unfortunately, (particularly in) the last couple of years. No industry and no organization or software company is immune."

Are impacted dealerships still selling cars?

Several major auto companies—including Stellantis, Ford and BMW—confirmed to The Associated Press last week that the CDK outage had impacted some of their dealers, but that sales operations continue.

In light of the ongoing situation, a spokesperson for Stellantis said Friday that many dealerships had switched to manual processes to serve customers. That includes writing up orders by hand.

A Ford spokesperson added that the outage may cause "some delays and inconveniences at some dealers and for some customers." However, many Ford and Lincoln customers are still getting sales and service support through alternative routes being used at dealerships.

"The people who've been around longer—you know, guys who have maybe a little salt in their hair like me—we remember how to do it before the computers," said John Crane of Hawk Auto Group, a Westmont, Illinois-based dealership operator that uses CDK. "It's just a few more steps and a little bit more time."

Although impacted Hawk Auto dealerships are still able to serve customers by "going back to the basics," Crane added that those working in administration are still "pulling out our hair." He notes that there are now stacks of paper awaiting processing—in place of orders that went through automatically on a computer overnight.

Group 1 Automotive Inc. said Monday that the incident has disrupted its business applications and processes in its U.S. operations that rely on CDK's dealers' systems. The company said that it took measures to protect and isolate its systems from CDK's platform.

In regulatory filings, Lithia Motors and AutoNation disclosed that last week's incident at CDK had disrupted their operations as well.

Lithia said it activated cyber incident response procedures, which included "severing business service connections between the company's systems and CDK's." AutoNation said it also took steps to protect its systems and data, adding that all of its locations remain open "albeit with lower productivity," as many are served manually or through alternative processes.

HOW CAN I PROTECT MYSELF?

With many details of the cyberattacks still unclear, customer privacy is also at top of mind—especially with little known about what information may have been compromised this week.

If you've bought a car from a dealership that's used CDK software, cybersecurity security experts stress that it's important to assume your data may have been breached. That could potentially include "pretty sensitive information," Steinhauer noted, like your social security number, employment history, income and current or former addresses.

Those impacted should monitor their credit—or even freeze their credit as an added layer of defense—and consider signing up for identify theft monitor insurance. You'll also want to be wary of any phishing attempts. It's best to make sure you have reliable contact information for a company by visiting their official website, for example, as scammers sometimes try to take advantage of news about data breaches to gain your trust through look-alike emails or phone calls.

Those are some best practices to keep in mind whether you're a victim of CDK's data breach or not, Steinhauer said. "Unfortunately, in this day and age, our data is a valuable target—and you have to make sure that you're taking steps to protect it," he said.

© 2024 The Associated Press. All rights reserved. This material may not

be published, broadcast, rewritten or redistributed without permission.

Citation: Car dealerships in North America revert to pens and paper after cyberattacks on software provider (2024, June 24) retrieved 29 June 2024 from <https://techxplore.com/news/2024-06-car-dealerships-north-america-revert.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.