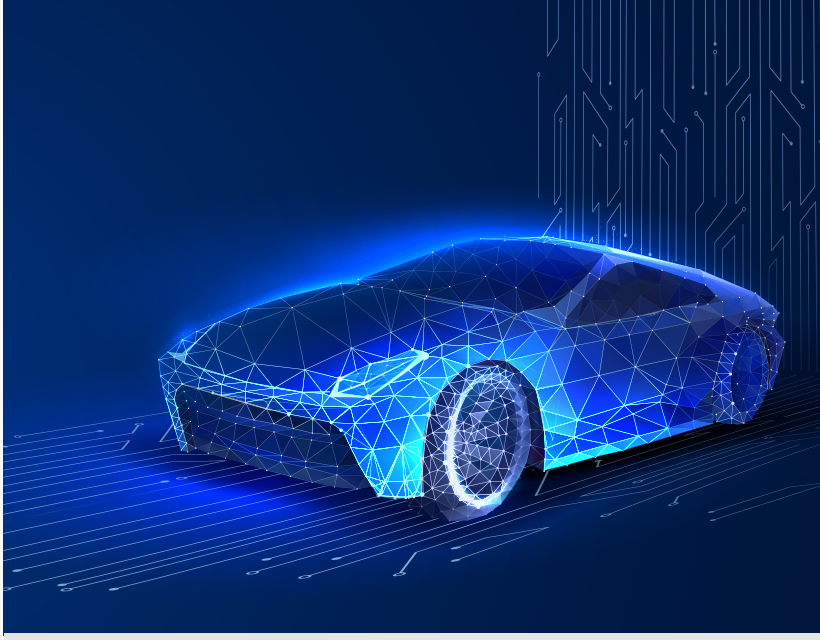
# This One Quarterly Action Can Transform Your Dealership Security



Berge Auto Group operates seven dealership locations with over 100 computers or servers at each location — plenty of devices for cyber criminals to target, and Berge Auto Group's Chief Financial Officer, Duane Wilkes, knows it.

"Data is one of the major assets of the company. It might not be on the balance sheet, but if you don't have that data — you can't put anything on the balance sheet," Wilkes said.

Berge Auto Group fortifies its defenses with quarterly vulnerability scans conducted by the expert team at One Step Secure IT, enhancing its readiness against potential threats.

"We felt it was very important to not only understand our systems from the view of a third party looking in but also to be able to create a roadmap to address what we need to work on," Wilkes said.

Conducting quarterly third-party vulnerability scans offers numerous advantages for dealerships:

Protecting Customer Data: Auto dealerships handle sensitive customer information, including financial data, driver's license information, and personal details. Vulnerability scans help identify weaknesses in the dealership's systems that could be exploited by hackers to access this data.

Compliance Requirements: Many auto dealerships are subject to regulatory requirements such as the Payment Card Industry Data Security Standard (PCI DSS) or the FTC Safeguards Rule. Regular vulnerability scans help ensure compliance with these standards, avoiding potential penalties and legal issues.

Protecting Business Operations: Cyber attacks can disrupt business operations, leading to downtime, loss of revenue, and damage to the dealership's reputation. By conducting vulnerability scans, auto dealerships can identify and address vulnerabilities before they are exploited by attackers, reducing the risk of costly disruptions to their business.

Maintaining Brand Reputation: Customers expect auto dealerships, to take security seriously and protect their sensitive information. A data breach resulting from unaddressed vulnerabilities can severely damage the dealership's reputation and erode customer trust. According to the CDK State of Cybersecurity in the Dealership, 84% of consumers said they would not go back to buy another vehicle after the personal data theyhad shared with a dealership had been compromised.

Identifying Third-Party Risks: Auto dealerships often rely on third-party vendors for various services, such as customer relationship management (CRM) systems, website hosting, or inventory management software. Vulnerability scans can help identify security risks associated with these third-party vendors, allowing the dealership to mitigate those risks through better vendor management or alternative solutions.

Overall, third-party vulnerability scans are an essential starting point for auto dealerships to proactively identify and address security risks.

Operating a dealership with weak security poses significant risks, potentially leading to costly and damaging consequences. Taking the small step of conducting a quarterly vulnerability scan can yield substantial benefits, significantly enhancing overall dealership security.

"We're tightening things up," Wilkes said after seeing the effects of third-party scans. "I can tell we've made a lot of improvement."