onestep
Secure IT Services

(623) 227-1997

8 STEPS FOR CYBER PROTECTION AFTER THE CDK BREACH

By Tim Derrickson, Director of IT & Security Services, CISSP and Kevin McAdam, CRO

The recent CDK breach is a significant blow to the automotive industry, affecting dealerships and individuals alike. As a cybersecurity managed services provider, we are committed to safeguarding people's livelihoods from such relentless cyber threats. In response to numerous inquiries about protecting against further damage, we are sharing eight crucial steps every dealer should take.

While some of these steps may seem technical, a sophisticated approach is necessary to counter the advanced methods now used by cyber criminals. The era of relying solely on basic cybersecurity tools is over. Today, skilled labor is essential. We are here to assist if needed.

THE 8 STEPS TO TAKE

1. Change Passwords Immediately

Stolen credentials are a primary way attackers gain access. If you suspect a breach, change all important passwords immediately. Regularly rotate passwords every 90 days, as required by most compliance standards.

2. Secure VPNs

An open or always-on VPN is a significant risk. Ensure your VPN is up to date and only open it as needed. If there is not a compelling business reason to keep it open, close it down.

3. Conduct Phishing Training

Phishing training is crucial, especially after a breach. The CDK attackers likely have access to email and contact information, increasing the likelihood of sophisticated phishing campaigns. A recent critical security vulnerability in Microsoft 365 uncovered this week further underscores the importance of vigilance against phishing. This vulnerability allows attackers to send spoofed emails appearing to come from Microsoft employees. This creates a deceiving phishing method that affects all Outlook accounts and significantly increases the risk of supply chain attacks.

4. Apply Defense in Depth

Assume that breaches are inevitable., The CDK attack reinforces this understanding. Defense in depth means having multiple layers of security to contain threats. Just having an EDR (Endpoint Detection and Response) or MDR (Managed Detection and Response) isn't enough. For example, these 2 security practices should be implemented to strengthen your defenses:

- **Service Path Security:** Ensure service paths are properly escaped to prevent executables from running. These will often recur after system updates and therefore must be regularly scanned for and corrected.
- **Elevated Privileges:** Monitor and secure accounts with elevated privileges.

5. Defend Both North-South and East-West

Cyber threats often involve infiltrating networks (north-south) and moving laterally (east-west). Implementing both north-south and east-west defenses ensures comprehensive security. North-south defenses secure the network perimeter, while east-west defenses monitor internal traffic to prevent lateral movement.

6. Monitor Alerts Effectively

Deploy tools like EDR (Endpoint Detection and Response) or MDR (Managed Detection and Response) and ensure skilled personnel are monitoring and responding to alerts. Timely patching and alert monitoring are vital to prevent breaches. Having your skilled labor on point in the coming weeks is vital.

7. Know Your Vulnerabilities

Assume criminals have accessed your environment. Understand the potential damage and take action to mitigate risks. Schedule vulnerability assessments with a credentialed third-party security team to identify and address vulnerabilities. This could be a level 1 test or a level 3 test. The next 3 weeks are going to be telling as to how deeply the criminals responsible for the CDK breach infiltrated the dealerships.

8. Review Your Cyber Liability Policy

Ensure your cyber liability policy is up to date, provides adequate coverage, and that your dealership complies with policy requirements. Non-compliance can lead to voided policies after an incident. Ensure your coverage is sufficient for both first- and third-party damages.

The CDK breach is a severe attack and it will have long-lasting impacts. Dealers must take proactive steps to protect themselves. Beyond these 8 cybersecurity measures, having a team of qualified security professionals is crucial. The first element of a robust information security program, and point 1 from FTC Safeguards, is **"designate a qualified individual to implement and supervise your company's security program".** This step is often overlooked but is vital for effective protection.

ABOUT ONE STEP SECURE IT

Since 1985, One Step has empowered businesses nationwide to leverage technology for competitive advantage, focusing on growth and revenue.

Specializing in cybersecurity, managed/co-managed IT, information security, and compliance services, we adapt to evolving customer needs and emerging threats.

Based in Phoenix, Arizona, we serve clients nationwide.

Learn more at **www.onestepsecureit.com.**

CONTACT US

Tim Derrickson
tderrickson@onestepsecureit.com

Kevin McAdam
kmcadam@onestepsecureit.com