Investigation and Research Report

The CDK Global Outage

Prepared by: Esther Ogunlana
Date: November 9, 2024

Executive Summary

According to BleepingComputer, a notorious extortion organization called the BlackSuit ransomware gang carried out a cyberattack on CDK Global on June 19. CDK Global, a leading provider of dealership management systems and other technology solutions for the automotive industry, fell victim to a ransomware attack that disrupted its operations and affected its clients.

The attackers used sophisticated methods to infiltrate the company's systems and encrypt data, demanding a ransom for its release. The attack resulted in operational disruptions, significant financial losses for affected dealerships, and a broader impact on the automotive industry. This report explores the details of the CDK Global ransomware attack, including the methods used, the victims involved, the motivations behind the attack, and recommendations for mitigating such risks in the future.

Introduction

A cyberattack refers to any deliberate attempt to steal, expose, modify, disrupt, or destroy data, applications, or other resources by gaining unauthorized access to a network, computer system, or digital device.

Cyber attackers, or threat actors, are motivated by a wide range of reasons, from personal gain to political or military objectives. They employ various techniques, such as malware, social engineering, and password theft, to infiltrate and compromise their targeted systems (IBM, 2024).

Cyberattacks, especially ransomware incidents, continue to pose significant threats to businesses worldwide. The CDK Global ransomware attack highlights the vulnerability of critical industries, such as automotive technology, to such attacks. The breach disrupted operations for several weeks and underscored the need for robust cybersecurity measures in enterprise networks, especially in sectors with extensive customer data and operations. This report examines the specifics of the attack, including the perpetrators' motives, the attack's impact, and how organizations can defend against such threats.

Attack Details

The Attack: CDK Global provides clients in the auto industry, a SaaS platform that handles all aspects of a car dealership's operation, including CRM, financing, payroll, support and service, inventory, and back-office operations.
The cyberattack began on June 19, causing widespread outages to CDK’s dealership customers. CDK confirmed it experienced an additional cyberattack later in the day that it said was likely to result in extended outages. It’s unclear if, or how, the second cyberattack was related to the first.
Car dealership software-as-a-service provider CDK Global was hit by a massive cyberattack, causing the company to shut down its systems and leaving clients unable to operate their business normally.

Victims of the Attack: CDK Global's primary victims were the company itself, its employees, and its automotive dealership clients who relied on the company's software and IT services. CDK Global's dealership management systems, which include sales, service, and parts management, were heavily impacted, causing disruptions at dealerships that depend on the system for day-to-day operations.

Technologies and Tools Used: The ransomware attack on CDK Global is believed to have been carried out using REvil ransomware, a notorious variant known for encrypting files and demanding large ransom payments. The attackers infiltrated CDK Global's network by exploiting vulnerabilities in their systems, possibly using phishing emails or remote desktop protocol (RDP) attacks to gain unauthorized access. Once inside, the ransomware encrypted critical files, making systems inoperable, and a ransom demand was made to restore access to the encrypted data.

Timeframe: The ransomware attack occurred in July 2021, with the first signs of a breach appearing when CDK Global began experiencing disruptions to its network and services. The attack's full impact was realized over the next several weeks as systems remained offline or were affected by the encryption of files.

Systems Targeted: The attackers primarily targeted CDK Global's dealership management systems, which are used by automotive dealerships to manage everything from sales and inventory to customer data. These systems are critical for the operation of many dealerships, making them high-value targets for cybercriminals. The attack also impacted the company's internal systems, including employee communications and financial data management.

Motivation and Objectives: The attackers, believed to be part of a cybercrime group using REvil ransomware, were likely motivated by financial gain. The attackers demanded a ransom in cryptocurrency, which is a common tactic used in ransomware attacks. By encrypting critical data and locking the systems of an essential industry player, the attackers aimed to extort money from the company, likely capitalizing on the fact that CDK Global's clients would face significant operational disruptions without access to their systems.

Outcome of the Attack: The outcome of the CDK Global ransomware attack was a disruption of services for many automotive dealerships that relied on the company's software for their day-to-day operations. The encrypted systems meant that employees at dealerships could not access customer data, sales records, or inventory information. Several dealerships were forced to resort to manual processes, which led to operational delays, financial losses, and reputational damage. The extent of the ransom payment and whether it was made is unclear, but the incident certainly resulted in recovery costs and increased cybersecurity spending for the company and its clients.

Mitigation and Recommendations

Security Controls

Regular Patch Management: Implement a stringent patching and update protocol to ensure that known vulnerabilities in software and systems are addressed immediately. This includes the timely application of security patches to both operating systems and applications.

Multi-Factor Authentication (MFA): Use MFA to protect access to critical systems, especially for remote access methods like RDP. This would help mitigate unauthorized access to systems, even if login credentials are compromised.

Network Segmentation: Segment the network to ensure that critical systems are isolated from general business networks. This can limit the spread of malware and ransomware once the attacker has breached the network perimeter.

Backup Systems: Regularly back up critical data and ensure that backups are stored offline or in a secure cloud environment. This ensures that organizations can recover quickly from ransomware attacks without paying the ransom.

Employee Training and Awareness: Conduct ongoing training for employees to recognize phishing attempts, malware, and social engineering tactics. Since human error is often the entry point for ransomware, proper training can reduce the likelihood of an attack succeeding.

Post-Attack Recovery: Following the attack, CDK Global and its clients should have implemented a robust incident response plan, including:

Forensic Investigation: Conduct a thorough investigation to determine the attack vector, how the attackers gained access, and any data that may have been exfiltrated.
Communication Strategy: Ensure that all affected parties are notified promptly, including customers and regulators, to minimize reputational damage.

Security Posture Review: Reassess and improve cybersecurity measures across the board, focusing on areas that may have been exploited by the attackers (e.g., RDP access, unpatched systems).

Conclusion

The CDK Global ransomware attack highlights the significant vulnerabilities that organizations in critical industries face, particularly when their systems are relied upon by third-party businesses. This attack serves as a reminder of the importance of proactive cybersecurity measures, including network segmentation, regular patching, and employee training. By implementing these security practices, organizations can reduce their risk of falling victim to ransomware attacks and ensure quicker recovery if an incident occurs.

References

Abrams, L. (2024, June 20). *CDK global cyberattack impacts thousands of US car dealerships*. BleepingComputer. https://www.bleepingcomputer.com/news/security/cdk-global-cyberattack-impacts-thousands-of-us-car-dealerships/

Beaty, A. (n.d.). *Cdk reportedly paid $25 million to end US car dealership cyberattack: 3 things you should know*. ZDNET. https://www.zdnet.com/article/us-car-dealerships-are-recovering-from-massive-cyberattack-3-things-you-should-know/

Ibm. (2024, October 1). What is a cyberattack? IBM. https://www.ibm.com/topics/cyber-attack

Abrams, L. (2024b, June 24). *CDK global outage caused by BlackSuit ransomware attack*. BleepingComputer. https://www.bleepingcomputer.com/news/security/cdk-global-outage-caused-by-blacksuit-ransomware-attack/

Whittaker, Z. (2024, June 27). Car dealership outages drag on after Cdk Cyberattacks. TechCrunch. https://techcrunch.com/2024/06/24/car-dealership-outages-drag-on-after-cdk-cyberattack/