executech

Rescuing A Company From Ransomware

How a family-owned auto dealership recovered from a costly ransomware attack by making the switch to Executech

Introduction

About the Client

Allied Autos* is a family-owned auto dealership group that sells and services trucks throughout the Intermountain West. With over a dozen locations spanning across four states, Allied Autos has received numerous awards in the trucking industry, including "Dealer of the Year." By 2018, Allied Autos had grown to over 300 employees. Prior to becoming an Executech client, the company had relied on a small internal IT team to handle their technology needs.

About Executech

Executech is an award-winning, outsourced IT services provider. Executech is one of the largest providers of enterprise-quality IT to small and medium-sized organizations in the West. Over the last 20 years, thousands of organizations have entrusted Executech to provide critical IT support, cloud services, and security solutions.

**Name of business has been changed to protect identities.*

The Challenge

A Ransomware Attack

In 2019, the CFO of Allied Autos approached Executech with a problem: several of his employees' computers had been hit by ransomware. One of the employees had accidentally clicked on a malicious pop-up, which allowed hackers to access their servers and implement ransomware. As a result, the company's employees could not access important files without having to pay a ransom fee.

No Fee, No Files

Allied Autos' internal IT team had not been able to detect or prevent the hack, and to make matters worse, they had not been conducting regular data backups.

Having heard of Executech's strong reputation for enterprise-quality IT services, the CFO at Allied Autos quickly called them to conduct a risk assessment.

First Response

Executech Conducts a Comprehensive Assessment

Working quickly and closely with the internal IT team at Allied Autos, Executech's consultants evaluated the state of the company's network security. Following the assessment, they met with the CFO and internal IT team at Allied Autos and recommended the following:

1: Upgrade to Microsoft 365 - Microsoft 365 licenses include advanced security protections, particularly for email.

2: Install New Firewalls - New firewalls, equipped with more advanced network filtering settings, can dramatically increase security and network efficiency.

3: Install Anti-Ransomware - Leading anti-ransomware software installed on all endpoints will use machine learning to identify potential risks and stop viruses before they reach a network.

4: Implement Better Backups - Correctly configured backups are key to good network security. While Allied Autos did have a backup in place, it was not setup correctly to be helpful in the event of a cyber attack.

These were best practices that Executech recommended based on years of experience helping clients address cybersecurity attacks. Allied Autos' internal IT staff valued the advice since they had limited experience with cybersecurity.

The Second Challenge

Return of the Ransomware

Just two days after Executech presented their recommendations, Allied Autos was **hit again by ransomware**. Allied Autos' internal IT team had not yet decided on implementing the recommendations nor had time to start any of the fixes needed from the first attack.

Despite the efforts of their internal IT team, the ransomware attackers had found a way to gain **access to the servers**. This time, it was through a local service provider that Allied Autos used for server management services. A virus had captured this service providers' login credentials, and once again, the company found itself unable to access critical files due to the ransom.

The ransomware attack had a significant financial cost: Allied Autos lost two weeks' worth of accounting work that needed to be re-done, as well as product photos and warranty contracts that were critical for serving their customers. In total, this lost data **cost the company over $25,000**.

> This time, the CFO of Allied Autos knew he needed a more reliable solution, fast.

Allied Autos called Executech again, who immediately sent in a dedicated team to save the company's network and implement all of the recommended technologies and security practices.

Solution

Executech Saves the Day

Executech immediately sent in a team of five technicians to remediate and repair the company's IT system.

- Over the next 24 hours, Executech installed anti-virus and anti-ransomware endpoint protection on 320 devices across the client's 14 locations.

Executech's team also found the computer that was originally responsible for spreading the ransomware – a device that had been previously overlooked by the internal IT team. Within two business days:

- Executech completed a total overhaul and upgrade of their cybersecurity defenses

Executech's work allowed Allied Automotive's employees to return to business as usual with an increased layer of protection and data backups.

Impact

The Executech Peace-of-Mind

Today, Allied Autos enjoys a secure network, protected by a state-of-the-art firewall, email filtering system and antivirus, all being managed by Executech consultants who are available 24/7, 365 days a year. The company no longer faces the constant risk of sensitive data being accessed and exploited, and the owners of Allied Autos can focus on growing their business with the peace-of-mind provided by Executech's world-class service.

Allied Autos is now a proud client of Executech, which has replaced their internal IT team to support the Company's ongoing growth. Executech now provides Allied Autos with not just managed security services, but managed IT support and managed cloud services as well.

FROM THE CUSTOMER:

> As CFO of one of the largest dealer groups in the nation, I realized that the weakest element of our executive management team was our knowledge of technology and the ongoing need for managed security. Now that we have engaged Executech, I can sleep at night knowing we are in good hands.

- TOM ANDERSON*

CFO | Allied Autos

**Name of client and business owner have been changed to protect identities.*

Get access to Executech's world-class suite of managed security services through our new Threat Detection & Prevention Essentials package.

LEARN MORE >

Receive a free assessment and learn how Executech can protect your business from cyber-attacks and data breaches.

PROTECT YOUR BUSINESS >

Get In Touch:

800.400.7554

Utah Headquarters
1314 W 11400 S
South Jordan, UT 84095

executech