Auto Dealers Under Imminent Threat of Security Breaches, Helion Technologies Announces

TIMONIUM, MD, UNITED STATES, August 22, 2016 /EINPresswire.com/ -- Helion Technologies announced today that 75 percent of small businesses have experienced security breaches in the last 12 months, according to a recent survey conducted by Osterman Research. The findings were published in a July 2016 report titled IT Security at Small to Mid-Size Businesses (SMBs): 2016 Benchmark Survey. The results were obtained from organizations ranging in size from 100 to 3,000 employees.

Helion Logo

"These findings are similar to what we are seeing in auto dealerships, and unfortunately we are seeing the rates of attack continuing to increase," said Erik Nachbahr, President of Helion Technologies. "Every time a hacker successfully breaches a network and profits from the attempt, 10 more hackers get into the game."

> These findings are similar to what we are seeing in auto dealerships, and unfortunately we are seeing the rates of attack continuing to increase
>
> *Erik Nachbahr, President of Helion Technologies*

Small businesses, defined as having fewer than 500 employees, were most vulnerable to security attacks as they are less likely to have full-time security experts on staff. Nearly one-third of the survey respondents have two or fewer IT personnel focused solely on security, indicating that smaller companies do not have the expertise necessary to deal with attacks, infections and other problems quickly and efficiently.

"Security doesn't have to be this massive, complicated problem for auto dealers," said Nachbahr. "Prevention is actually pretty inexpensive and easy. What's really costly is when a breach happens. A single incident may result in the loss of hundreds of thousands of dollars. Yet with simple technology precautions as well as employee awareness and training, these incidents can easily be prevented."

According to the survey, the most successful form of security attacks included:

Phishing: 43 percent of SMBs experienced a successful phishing attack. Phishing attacks appear in the form of emails that appear to come from a legitimate entity or person, such as a bank. The message contains a link that takes the victim to a fraudulent website; for example, a website that looks exactly like the bank's website. The user is prompted to provide login information, which is then used by the hackers to access the dealerships' real bank account.

Spear phishing takes the scam one step further and targets specific individuals within organizations.

In auto dealerships, typically this is the controller or someone in the accounting office. The employee receives an email that appears to be from a dealer principal or general manager, with a request and instructions on how to wire money to an account. Once the money is wired, there is no way to retrieve it.

Virus or Worm Infection: 36 percent of SMBs experienced these types of attacks, which are computer codes that replicate themselves and spread through a computer network. Viruses and worms are designed to destroy data, use available memory and bring systems to a halt.

Ransomware: 23 percent of SMBs were victims of ransomware, a type of malware that infects computer networks and lies dormant for a period of time. Once activated, ransomware encrypts all files in an organization and the hackers demand a ransom for their release.

The survey also found that for SMBs, overall security-related costs have increased an average of 23 percent in the last 12 months. The increase is likely correlated to the growing number of security threats; for example, in 2015 the number of phishing URLs increased by 55 percent and the total volume of new malware increased by 14 percent.

One of the primary targets in SMBs is data. In auto dealerships there is enormous value in all of the customer records kept in dealership management systems and customer relationship management applications. Stolen login credentials, credit card numbers, social security numbers and account numbers can be used for a variety of purposes; including gaining access to corporate financial accounts, selling credit card numbers on the open market or creating new identities for criminals.

Auto dealership employees can minimize the threat posed by phishing, worms, viruses and ransomware by doing the following:
• Don't click on any links in emails or download documents sent by an unknown party
• If you receive an email from your bank, don't use that link to go to the bank's website. Instead open a new window to navigate to your bank's website. If you have any concerns about the content of the message you received, call your bank
• Require verbal authorization for all email requests to wire or transfer money
• Keep every computers' operating system and other software applications up to date, installing patches and updates regularly
• Use firewall and antivirus software

For more information contact Helion at 443-541-1500 or visit http://www.heliontechnologies.com.

About Helion Automotive Technologies

Helion...Putting Your Dealership in the FAST LANE! Helion Automotive Technologies is a leading IT solutions provider, providing auto dealers with faster, more efficient networks and secure data protection. From managed services to IT assistance and service desk help, Helion offers both short-term IT fixes and long-term planning so dealers can focus on what matters most: selling more cars. Helion has specialized in IT for more than ten years and works with 650+ auto dealers nationwide. Dealers can request a free assessment of their IT needs at www.heliontechnologies.com.

Holly Forsberg
Carter West Public Relations
602-680-8960
email us here
