The Biggest Security Threat to Auto Dealerships is the Employees, Warns Helion

TIMONIUM, MD, UNITED STATES, March 21, 2016 /EINPresswire.com/ -- Helion Automotive Technologies, a leading provider of information technology (IT) solutions to auto dealerships, warns that the biggest security threat to auto dealerships is the employees. International crime organizations are targeting auto dealers, among other service businesses, with sophisticated and targeted email scams designed to trick unwitting employees into performing actions that make dealership networks vulnerable to attack.

"The increase in the number of organized attacks in the last year is astounding and auto dealers need to be on alert," said Erik Nachbahr, President of Helion. "In addition to the volume of attacks, the level of sophistication and research involved is frightening. Remember the emails from the dethroned princes from Nigeria? Hardly anybody fell for those, but many employees are falling for the tactics being used today."

Dozens of auto dealerships across the country have already fallen victim to hackers who have successfully managed to access the following information:

> Remember the emails from the dethroned princes from Nigeria? Hardly anybody fell for those, but many employees are falling for the tactics being used today.
> *Erik Nachbahr, President*

- Auto dealerships' bank account numbers, routing numbers and login credentials
- Customers' bank account numbers and routing numbers
- Customers' credit card numbers, addresses, social security numbers and credit scores

Employees who work in the accounting department and F&I departments are most at risk for being targeted by sophisticated email scams.

Here is a sampling of actual incidents:

A dealership controller received an email from someone who he thought was the dealer. The dealer requested a wire transfer of $30,000. After a few emails back and forth, the controller complied with the request. Unfortunately, the bank was not able to retrieve the $30,000.

A virus was downloaded in an email attachment onto the F&I Manager's computer. The virus tracked every website visited and every keystroke. Hackers were able to use the information to login into credit bureau sites and extract credit reports for over 200 customers before they were caught. This

incident ultimately cost the dealer more than $150,000.

An accountant was tricked into visiting what he thought was Bank of America's website. The accountant was prompted to enter in login information, bank account numbers and other information that enabled hackers to initiate a $400,000 wire transfer. Fortunately, the real Bank of America was able to stop the transfer before it happened.

Another tactic growing in popularity is to install a virus that encrypts every file on the network. Hackers then demand a ransom to release the files back to the business. Small businesses in the U.S. and Europe have already paid out hundreds of thousands, if not millions of dollars to these hostages, because they don't have much of a choice. It's either pay up, or their business is shut down.

Security software and firewalls can't stop these types of attacks, because they all originate from emails that are sent to employees. And, these are not random emails that are flagged as spam. They are targeted attacks on specific dealerships and the individual employees who work there. Attackers create "from" email addresses that closely resemble the domain name and employee names within that organization.

According to Symantec, half of all spear phishing attacks (emails to employees that contain viruses, malware and links to fake websites) target small businesses, defined as 1 to 250 employees. The most targeted industries are finance, insurance, real estate and the services sector.

To help defend against spear phishing attacks, Nachbahr makes the following recommendations to dealers:

1) Verbally verify all requests for wire transfers

2) Be sure to have the right cyber-liability insurance policy in place. The majority of dealerships do not have cyber-liability insurance coverage, which is concerning. It's not a matter of if dealerships will experience a cyberattack, but when.

3) Employee training. Be sure your employees know the latest cyberwarfare tactics, and how to combat them.

4) Keep software patches updated. Nachbahr estimates that more than 90 percents of dealerships do not have a system in place to keep their patches updated on a regular basis. This is like leaving your back door open at night - a virtual invitation to cyberthieves.

To learn more about the latest security threats to your dealership, contact Helion at 443-541-1500.

Or, stop by Helion's booth # 5816N at NADA. To make an appointment visit http://bit.ly/1Q3sHa9.

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 http://www.heliontechnologies.com.

Holly Forsberg
Carter West Public Relations

6026808960
email us here