UVSA

UNITED VETERINARY SERVICES ASSOCIATION
The Pulse of the Industry

For Immediate Release (August 29, 2022)

Ransomware attacks have severely impacted the animal health care industry, prompting The United Veterinary Services Association (UVSA) to take immediate action.

The United Veterinary Services Association (UVSA) has created Cybersecurity "Best Practices" recommendations to promote safe, efficient, and effective operations for distributors, manufacturers, and suppliers of animal care products. The recommendations come in the aftermath of a ransomware attack that impacted more than 700 animal health care networks around the globe. The recommendations are designed to prevent data breeches, financial fraud, and economic losses.

UVSA recommended Best Practices include:

1. **End User License Agreements (EULA)**: EULAs are now standard practice for those engaged in B2B E-Commerce. EULAs should be in place for all users prior to allowing systems access.
2. **Site Access and Utilization Logging:** Logging the access and utilization of site customer credentialed activity is necessary for EULA compliance monitoring and notification to users in the event of EULA violations or the event of a potential security breach.
3. **Multi-Factor Authentication (MFA):** MFA is now a cybersecurity best practice for commercial and financial systems. Implementation of multi-factor authentication protocols should be in place as a required component for platform access.
    1. If full MFA implementation is not possible, consider requiring MFA for a subset of user actions focused on securing private party data (SSN, licensure information, etc.) and financial data (payment information, bank information, etc.).

    2. If full MFA implementation is not possible, consider using a CAPTCHA test to differentiate human vs. bot (machine) users for all access or to limit access to privacy/financial data (as described above).

4. **Third-Party Access EULA:** In the event a third-party requires access to provide an authorized business application, each third-party should execute a EULA prior to receiving systems access. Such access should then be delivered only through an approved application programming interface (API).
    1. A third-party EULA should clearly define acceptable platform use, limitations on platform use, security expectations for connected systems, security expectations for retrieved data, data usage limitations, and rights to audit access and data security/utilization.
    2. The API should allow access via unique third-party credentials and limit that access only to data required by the third-party for legitimate business operations. Use of the API can be subject to rate limits and data limits to ensure the e-commerce platform is not unduly loaded.

The “Best Practices” recommendations were developed by IronNet, a cybersecurity company engaged by the United Veterinary Services Association (UVSA) as a subject matter expert, based on the work of the UVSA Distributor Working Group on Cybersecurity.

The mission of UVSA is to be the hub for relevant information leading to innovation in the supply chain, and in so doing enable animal care by supporting those who serve the veterinary channel. The cyber security recommendations are designed to support and protect UVSA members. UVSA is a national trade association comprised of distributors, manufacturers, and suppliers of animal care products in the veterinary channel. www.uvsa.net

Interview Availability:

- UVSA Board of Directors Chairwoman Betsy Watkins, PRN Pharmacal
- Photos are available upon request for media usage

MEDIA CONTACT:
Kathleen Cairns, Communications Strategist
Fallston Group
443-714-4836
Kathleen.Cairns@fallstongroup.com