KISTERS

Erklärung für eine sichere IFAS - Software

Sehr geehrte Damen und Herren,

wie Sie von uns wissen, gab es bei uns im Haus einen IT Sicherheitsvorfall. Als Sofortmaßnahme haben wir vorsorglich alle Systeme vom Netzwerk getrennt und isoliert geprüft.

Wir möchten Ihnen heute mitteilen, dass es nach aktuellem Stand der forensischen Untersuchungen keine Anhaltspunkte dafür gibt, dass unser Entwicklungsnetzwerk, welches für die Entwicklung von KISTERS-Lösungen genutzt wird, mit den entsprechenden Sourcen und Build-Umgebungen, von diesem Angriff betroffen ist.

Zur weiteren Absicherung haben wir folgende Maßnahmen durchgeführt:

1. Die Dateien der letzten Auslieferungen für unsere Software Lösungen liegen in separaten Repositories. Diese Repositories wurden von unserem Build-System getrennt und einzeln mit mehreren Scannern auf Befall von schädlicher Software geprüft. Es konnte kein Befall festgestellt werden. Das heißt alle bis zum Cyberangriff ausgelieferten Softwarestände gelten damit nach Stand der Technik als frei von Schad-Software und können somit produktiv weiterverwendet werden.
2. Der Datenbestand wurde ohne Befund auf auffällige Veränderungen innerhalb der letzte 3 Monate überprüft.
3. Für die Erstellung zukünftiger Patches und Updates haben wir unsere Build Systeme vorsichtshalber vollständig neu aufgebaut. Die Build Pipeline residiert jetzt wie vorher auf dedizierten und abgeschotteten Rechnern, die nur für das Erstellen der Binaries genutzt werden. Eine allgemeine Benutzeranmeldung ist hier nicht möglich.
4. Die Richtlinien auf unseren Entwicklungssystemen verhindern die direkte Anmeldung des Administrators (root) auf allen Systemen. Es ist zuvor eine Anmeldung mit einem lokalen Benutzer notwendig, der durch separate Passwörter abgesichert ist. Unsere Überprüfung ergab hier keine verdächtigen Anmeldungen innerhalb der letzten 3 Monate.
5. Unsere Arbeitsrechner und Server wurden vollständig neu installiert und sind mit aktuellsten sauberen Installationen neu hochgezogen worden. Alle Firewalls sind neu aufgesetzt und neu parametriert worden.

Aus diesem Grund sind zeitnah wieder alle unsere Systeme voll einsatzfähig und wir sind in der Lage Sie wieder sicher mit notwendigen Patches zur Behebung von kritischen Fehlern und demnächst auch mit Softwareerweiterungen und neuen Lösungen bedienen zu können.

Duisburg, den 26.01.22

Dr. Marcus Lempert

Head of Business Unit EHS
KISTERS AG