Manipulationssicher

Bildschirmschreiber setzten beim Erfassen von Daten auf Sicherheit

Michael Brosig,
Jumo

Ein Bildschirmschreiber kann wohl nicht alle Cyber-Security-Probleme dieser Welt lösen, aber durch ausgereifte Technik kann er dafür sorgen, dass die Prozesse, die durch ihn überwacht werden, für den Anwender eine „sichere Sache“ sind.

Im Jahr 1986 gelang Personal-Computern endgültig der Durchbruch auf dem Markt: So etwas wie ein Türöffner war der Intel 8036 Chip, der erste 32-Bit-Prozessor, der zusammen mit einer angepassten Windows-Version ein neues Computerzeitalter einläutete. 1986 war in der Computer-Geschichte aber noch aus einem anderen Grund eine Zeitenwende. Mit „Brain“ tauchte der erste PC-Computervirus auf. „Brain“ befiel lediglich Diskettenlaufwerke und verlangsamte diese. Eigentlich nur ein harmloser Scherz, der aber den Beginn einer neuen, unheilvollen Ära markierte. Denn seit diesem Zeitpunkt müssen sich auch Endverbraucher mit dem Thema „Computersicherheit“ auseinandersetzen.

Cyber Security aktueller denn je

32 Jahre später ist das Thema „Cyber Security“ aktueller denn je und die Zahlen sind mehr als erschreckend. Das AV-Test-Institut hat im letzten Jahr insgesamt 1 Mrd. Malware-Programme erfasst, die weltweit im Umlauf sind. Jeden Monat kommen zwischen 8 und 10 Mio. neue Programme dazu.

Auch die Zahl der gezielten Cyber-Angriffe steigt exponentiell. So registrierte die Telekom bspw. schon im April 2019 rund 46 Mio. tägliche Angriffe auf ihre 3.000 genannten „Honeypots“. Das sind so etwas wie digitale Fallen im Internet, die mit scheinbar interessanten oder wertvollen Inhalten potenzielle Cyberkriminelle ködern. Jeder Honeypot wurde also in einem Monat rund 15.000-mal angegriffen, das heißt 500-mal an jedem Tag.

Ist es überhaupt möglich, vor dem Hintergrund dieser Zahlen an ein halbwegs funktionierendes „Internet der Dinge“ zu denken? Können sich Unternehmen überhaupt wirksam schützen? Vor allen Dingen, wenn man bedenkt, dass der größte Unsicherheitsfaktor nach wie vor der Mensch ist. Wie schnell wird ein scheinbar harmloser Mailanhang angeklickt oder ein USB-Stick von einer Messe in den Firmenrechner eingesteckt?

◀ **Abb. 1: Der neue Bildschirmschreiber Jumo Logoscreen 700**

Lange Historie in Sachen Datenerfassung

Die in Fulda ansässige Firma Jumo hat eine lange Historie in Sachen Datenerfassung. Bereits 1964 brachte das Unternehmen den erste Papierschreiber auf den Markt. Diese Geräte lieferten – quasi

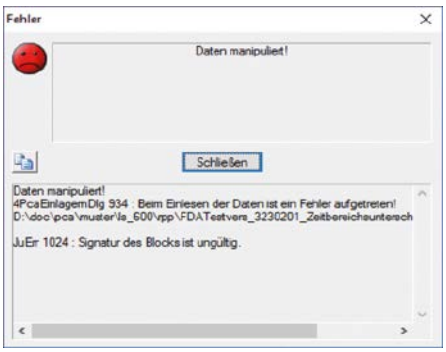

Abb. 2: Manipulationen werden sicher erkannt

Abb. 3: Beispiel eines digitalen Gerätezertifikats.

als analogen Output – einen bedruckten Papierstreifen. Die Frage nach der Manipulationssicherheit stellte sich damit gar nicht, denn jeder Eingriff wäre sofort sichtbar gewesen.

Das änderte sich mit den ersten Bildschirmschreibern. Die Messwerte, die diese erfassten, wurden nicht mehr auf Papier gespeichert, sondern als Daten auf einer Festplatte oder einem anderen Speichermedium und Daten sind bekannterweise manipulierbar.

Jumo hat sich deshalb bei den Bildschirmschreibern von Anfang an mit dem Thema „Manipulationssicherheit“ befasst. Bei neuem Top-Modell, dem Jumo Logoscreen 700, spielt dieses Thema natürlich auch eine zentrale Rolle. Zumal dieser Bildschirmschreiber eine FDA-konforme Datenerfassung ermöglicht. Die „Food and Drug Administration“ (FDA) ist die Lebensmittelüberwachungs- und Arzneimittelbehörde der Vereinigten Staaten und stellt besonders hohe Ansprüche an verwendete Materialien oder technische Prozesse.

FDA Anforderungen

Mit dem „21 CFR part 11“ formuliert die FDA Anforderungen an elektronische Aufzeichnungen und Unterschriften. Der 21 CFR part 11 findet immer dann Anwendung, wenn Informationen elektronisch erzeugt, verändert, gespeichert, übertragen oder auf diese zugegriffen werden sollen. Dabei kann es sich um die verschiedensten Typen an Informationen handeln wie bspw. Texte, Bilder, Videos oder Audiodateien

Diese Anforderungen sind dann zu erfüllen, wenn die damit erzeugten, gespeicherten, übertragenen oder veränderten Dokumente dazu dienen, die Einhaltung regulatorischer Vorschriften nachzuweisen wie bspw. Freigabe- und Testprotokolle Verfahrens- und Arbeitsanweisungen oder eben Aufzeichnungen aus der Produktion, wie sie mit Hilfe von Bildschirmschreibern erfasst werden. Der 21 CFR part 11 ist generell immer dann anzuwenden, wenn elektronische Aufzeichnungen das Papier ersetzen.

In diesem Fall gelten spezielle Anforderungen wie die Verschlüsselung von Dokumenten, digitaler Unterschriftenstandards, um die Echtheit, Integrität und Vertraulichkeit von Aufzeichnungen sicherzustellen.

Ddigitale Unterschrift

Um zu zeigen, wie akribisch die FDA bei diesen Themen vorgeht, lohnt sich ein Blick auf das Thema „Unterschriften.“ Eine digitale Unterschrift muss den Namen des Unterzeichnenden, das Datum und die Zeit der Unterzeichnung und die Bedeutung der Unterzeichnung (z.B. Review oder Genehmigung) enthalten. Diese Unterschrift darf nicht verfälscht werden können, muss mit dem Dokument so verbunden sein, dass sie nicht auf andere Dokumente angewendet werden kann, muss einem auch einem einzelnen Individuum zugeordnet werden können und muss oder aus zwei Komponenten wie Identifizierungscode und Passwort bestehen.

Der Jumo Logoscreen 700 kann all das leisten. Mit einem speziellen Typenzusatz verfügt das Gerät über eine TÜV-geprüfte Funktion zur Gewährleistung der Datensicherheit und erfüllt darüber hinaus alle FDA-Anforderungen zur papierlosen digitalen Prozessdatenaufzeichnung in der Pharma- und Lebensmittelindustrie.

Auf Basis eines digitalen Gerätezertifikats lässt sich nachweisen, dass die Registrierdaten nicht manipuliert wurden: weder im Gerät, noch während der Übertragung, noch bei der Auswertung. Dadurch hat der Anwender bei kritischen Audits einen sicheren Nachweis, dass keine Manipulation der aufgezeichneten Prozessdaten vorliegt

Die PC-Security-Manager-Software erlaubt die Verwaltung von bis zu 50 Benutzern pro Gerät. Eine elektronische Unterschrift kann für ein Chargenprotokoll, einen Zeitbereich, oder bei der Abmeldung zugewiesen werden. Die Vergabe von authentifizierten Kommentartexten am Gerät unterstreicht die Flexibilität beim Protokollieren von nachweispflichtigen Prozessen. Die Verwendung des digitalen Zertifikates sorgt auch hier für die sichere Manipulationserkennung.

Robuster Schutz gegen Manipulationsversuche

Der Gedanke dahinter ist einfach, aber bestechend. Da es immer schwieriger wird, eine Datenmanipulation zu verhindern, muss sichergestellt werden, dass jeder Eingriff sofort auffällt und nachverfolgt werden kann.

Das Fazit des TÜV-Berichts bestätigt dieses Konzept: „Die zweifache Prüfung der Integrität der Daten durch Prüfsumme und kryptographische Signatur bietet einen robusten Schutz gegen Manipulationsversuche. Auch die Prozedur zum Austausch von Gerätezertifikaten ist angemessen gegen Manipulationsversuche geschützt. Im Industrial IT Security Labor des TÜV Süd konnten keine Schwachstellen der durchgeführten Tests identifiziert werden.“

So kann ein Bildschirmschreiber wohl nicht alle Cyber-Security-Probleme dieser Welt lösen, aber durch ausgereifte Technik kann er dafür sorgen, dass die Prozesse, die durch ihn überwacht werden, für den Anwender eine „sichere Sache“ sind.

Der Autor

Michael Brosig, Pressesprecher, Jumo

Diesen Beitrag können Sie auch in der Wiley Online Library als pdf lesen und abspeichern:

https://dx.doi.org/10.1002/citp.202001216

Kontakt

Jumo GmbH & Co. KG, Fulda
Michael Brosig · Tel.: +49 661 6003-238
michael.brosig@jumo.net · www.jumo.net