CYBER-SECURITY-UPDATES FÜR ENCORE UND ENSUITE

MIT SICHERHEIT EIN GUTES GEFÜHL!

In einem immer stärker vernetzten Umfeld nimmt das Bewusstsein für sensible Informationen und deren sicheren Umgang kontinuierlich zu. Honeywell legt daher großen Wert auf das Thema IT-Sicherheit und entwickelt die bereits etablierte Technik ständig weiter.

Die aktuellen Versionen aller enCore-Mengenumwerter (FC1, ZM1, BM1) und enSuite stehen ganz in diesem Zeichen, die erhöhten Anforderungen an Cybersicherheit zu erfüllen. Weitere Geräteserien werden in Kürze folgen. Hier hat sich einiges getan und wenn Sie bereits enCore-Geräte einsetzen, werden Sie bei den neuen Versionen einige Veränderungen feststellen.

In diesem Artikel werden die technischen Hintergründe aufgezeigt und erläutert, die die Kommunikation mit den Geräten und den Zugriff auf deren Daten sicherer gemacht haben. Im Rahmen einer großen, konzernweiten Initiative wurden alle Aspekte unserer Geräte und Programme auf den Prüfstand gestellt. In diesem Zuge wurden auch einige der vorhandenen guten Konzepte überdacht und abermals verbessert – aber Sie werden sehen, dass sich für die tägliche Arbeit dadurch nicht viel ändern wird – für potenzielle Angreifer wird es aber schwieriger, Zugriff auf die Geräte oder sensiblen Daten zu erlangen. Aber wie überall im Netz kommt es primär darauf an, dass Sie als Anwender sich über Sicherheitsaspekte bewusst sind und die Schutzmöglichkeiten kennen und einsetzen.

WIE GERÄTE KOMMUNIZIEREN

Das Netzwerkprotokoll MMS (Manufacturing Messaging Specification nach ISO 9506) ist der wichtigste Kommunikationskanal der enCore-Geräte. Hierüber werden Parametrierungen übertragen, Archive abgerufen und vieles mehr. Ab sofort unterstützen die Geräte dieses Protokoll nur noch in Kombination mit einer nach TLS (Transport Layer Security) verschlüsselten Datenübertragung. Auf diese Weise wird verhindert, dass die Daten während der Übertragung mitgelesen oder gar manipuliert werden. Normalerweise befinden sich die Geräte für Anwendungen in der Gasversorgung in abgesicherten Netzen, aber es ist dennoch nicht auszuschließen, dass ein Unbefugter den Zugriff auf das Netz erlangt. Darum ist die Verschlüsselung ein großer Gewinn an Sicherheit.

Aber alles hat seinen Preis: Für eine funktionierende Verschlüsselung müssen die berechtigten Kommunikationspartner die Schlüssel besitzen und ggf. zunächst austauschen. Der Client (das PC-Programm enSuite) baut eine Verbindung zum Server (dem enCore-Gerät) auf, der sich gegenüber dem Client mit einem Zertifikat ausweist, das u. a. den öffentlichen Schlüssel des Servers enthält. Beide Teilnehmer können jetzt einen für diese Verbindung geltenden kryptographischen Schlüssel aushandeln, mit dem die weitere Kommunikation verschlüsselt wird.

In öffentlichen Netzen funktioniert das inzwischen automatisch, ohne dass der Nutzer etwas davon bemerkt: Nach Aufruf einer Internetseite im Browser ist die verschlüsselte Verbindung an einem grünen Schlosssymbol oder der URL, die mit https:// beginnt, zu erkennen. Das dabei ausgetauschte Zertifikat wird bei Servern im Internet von einer offiziellen Zertifizierungsstelle, der Certification Authority (CA), ausgestellt und kann vom Browser auch verifiziert werden. In den Bereichen, in denen die enCore-Geräte eingesetzt werden, gibt es (bisher) keine CA, da deren Betrieb einen nicht unerheblichen Aufwand bedeutet. Darum nutzen enCore-Geräte sogenannte selbstsignierte Zertifikate, die Überprüfung erfolgt durch den Anwender.

ZERTIFIKATE ÜBERPRÜFEN

Ein enCore-Gerät erzeugt bei der Inbetriebnahme oder nach Aufforderung ein Zertifikat, das auch am Gerätedisplay angezeigt werden kann. Bei der ersten Verbindung mit dem Gerät zeigt enSuite das empfangene Zertifikat an. Idealerweise prüfen Sie die Geräteseriennummer und den Fingerprint auf Übereinstimmung mit den am Gerät angezeigten Werten und klicken dann auf „Dauerhaft akzeptieren“. Ab jetzt werden Sie für dieses Gerät nicht mehr mit der Verschlüsselung und Zertifikaten behelligt, solange das Zertifikat nicht geändert wird (oder ein Angreifer ein anderes Zertifikat sendet).

SENSIBLE DATEN

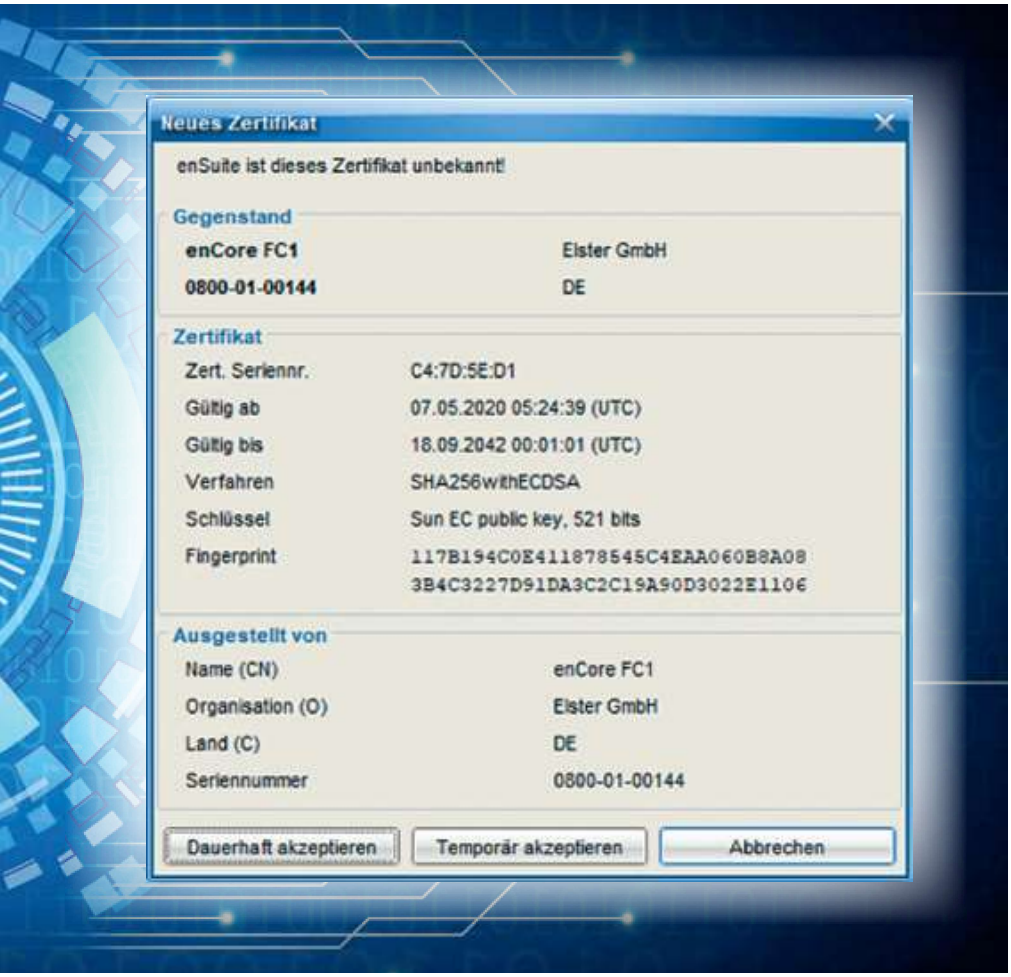
Ein weiteres Thema im Zusammenhang von Cyber Security ist der Umgang mit sensiblen Daten. Darunter werden Informationen verstanden, die einen Bezug zu einer Person haben (z. B. eine E-Mail-Adresse) oder Zugangsdaten wie etwa Passworte oder die PIN einer SIM-Karte. Bislang waren solche Daten in kleiner Zahl in Parametrierungen enthalten und konnten von jedermann eingesehen werden, der Zugriff auf die Parametrierung hatte. Ab jetzt gehen die Geräte und enSuite besonders sorgsam mit diesen Daten um: Die Daten sind weiterhin Bestandteil der Parametrierung, aber beim Auslesen einer Parametrierung werden sie nur authentifizierten, also angemeldeten Nutzern preisgegeben. Ohne Login kann die Parametrierung weiterhin gelesen werden, die sensiblen Daten sind aber nicht enthalten.

Wird die Parametrierung später wieder in das Gerät übertragen, dann bleiben die bereits im Gerät vorhandenen Einstellungen der sensiblen Parameter unangetastet.

Innerhalb des Gerätes werden die sensiblen Daten verschlüsselt gespeichert und stehen unter einem besonderen Schutz. Änderungen an sensiblen Daten sind nur mit gültigem Login möglich und im Änderungslogbuch wird nur die Veränderung mit Zeitstempel, nicht aber alter und neuer Wert protokolliert.

Die Parametrieroberfläche in enSuite markiert sensible Daten deutlich sichtbar mit einem grünen Schutzschild ( ) und erlaubt die Aktivierung der bereits erwähnten Funktion „beibehalten“. Beim Export einer bereits gespeicherten Parametrierung und beim Versenden via E-Mail gibt es jetzt die Option, die sensiblen Daten nachträglich entfernen zu lassen. So können Sie z. B. die Parametrierung bedenkenlos an Servicemitarbeiter weitergeben.

Doch bedenken Sie bitte: Als berechtigter Nutzer mit Login können Sie wie bisher alle Daten auslesen und in enSuite speichern. Sie sind also für die Sicherheit der sensiblen Daten auf Ihrem PC selbst verantwortlich! Wir empfehlen dringend, enSuite auf einem PC mit Festplattenverschlüs-



selung zu betreiben und Parametrierungen mit sensiblen Daten nur an vertrauenswürdige und berechtigte Personen weiterzugeben.

FERNBEDIENUNG – FERNES BEDIENFELD

Auch die Bedienung der Geräte aus der Ferne wurde sicherer gemacht.

Für die meisten Anwender unsichtbar: Die Kommunikation geschieht jetzt ebenfalls über das verschlüsselte MMS-Protokoll und nicht wie bisher über das unsichere HTTP. Das ferne Bedienfeld kann also nicht mehr mit einem einfachen Browser abgerufen werden. Damit wird das Mitlesen von Informationen durch Unbefugte wirksam unterbunden.

Deutlicher sichtbar ist jedoch folgende Veränderung: Es kann grundsätzlich nur ein Anwender das Gerät bedienen. Wenn also eine Fernbedienung stattfindet, dann ist die gleichzeitige Bedienung am Gerät nicht möglich. Es wird stattdessen eine Anzeige aufgeschaltet, die erklärt, wie man durch gleichzeitiges Drücken der beiden Funktionstasten die Fernbedienung beenden und die Kontrolle zurückerlangen kann.

Bei längerer Inaktivität (fünf Minuten) des fernen Benutzers wird die Bedienfeldverbindung automatisch unterbrochen.

Meistens findet die Fernbedienung statt, weil man sich den Weg in die Anlage ersparen möchte. In seltenen Fällen kann es aber vorkommen, dass zwei Personen tatsächlich den Displayinhalt sehen müssen, z. B. bei Hilfestellung durch Kollegen im Büro oder einen Servicemitarbeiter. Zu diesem Zweck kann der entfernte Nutzer in enSuite die Sichtbarkeit des eigentlichen Displays am Gerät erlauben. Er kann sogar die Bedienung am Gerät wieder freigeben und selbst weiterhin das Display beobachten. Die Verbesserung gegenüber früher: Jetzt liegt es in der Kontrolle der Anwender, wer wann welche Daten sehen kann.

Sobald der Benutzer am Gerät mit freigegebener Bedienung eine Eingabe per virtueller Tastatur tätigen möchte, wird dem entfernten Nutzer diese Eingabe verborgen, da er sonst in der Lage wäre, z. B. die Eingabe eines Passworts mitzulesen.

Wenn andererseits Sie als ferner Benutzer die Sicht auf das Display freigegeben haben und eine Eingabe tätigen möchten, dann können Sie selbst entscheiden, ob diese Eingabe am Gerät sichtbar sein soll. Für sensible Eingaben schalten Sie einfach kurz die Sichtbarkeit am Gerät ab.

FAZIT

Mit den neuen Versionen unserer Geräte haben wir die Voraussetzungen geschaffen, dass Sie Ihre Geräte sicherer betreiben und Ihre sensiblen Daten besser schützen können. Durch diese Verbesserungen können Sie jetzt also Mengenumwerter mit MID- bzw. innerstaatlicher Baumusterprüfbescheinigung einsetzen, die selbst hohe Anforderungen an Datensicherheit erfüllen.

Johannes Haas-Rollenbeck
johannes.haas-rollenbeck@honeywell.com