Smart Devices im Produktionsumfeld

Angriffsflächen von Alleskönnern

Industrieanlagen rücken immer mehr als verwundbare Systeme ins Bewusstsein. Berichte über Angriffe durch aufwändige und spezialisierte Schadprogramme wie Stuxnet[1], Duqu[2] und Flame[3] haben das Thema möglicher Schwachstellen in Produktionsanlagen stark hervorgehoben. Dabei ging es im Kern nicht nur um verwundbare Steuerungssoftware in SCADA-Systemen, oder um die Vernetzung kritischer Steuersysteme mit dem Internet, sondern auch um die innerbetriebliche Verzahnung von Steuerung und Fertigung mit der Unternehmens-IT. Dort erscheinen Smartphones, Tablets & Co. zunächst nur als ein weiteres mobiles Endgerät. Neben den notwendigen Schutzmaßnahmen gegen allgemeine Angriffe auf mobile Endgeräte verändert die Nutzung von Smart Devices jedoch auch entscheidend den Umgang mit Produktionsinformationen und deren Zugriffspfade.

Wie auch in anderen Bereichen bieten Smartphones, Tablets & Co. im Produktionsumfeld vielfältige Anwendungsmöglichkeiten für die Automatisierungs-, Steuerungs- und Wartungstechnik, auch bereits vor der Einführung von Konzepten wie Industrie 4.0[4]. Gerade für mobile Datenvisualisierung und Überwachungsaufgaben aus dem Bereich der Industriesteuerung besteht der Wunsch nach Lösungen, die für höhere Flexibilität beim Einsatz von Technikern durch Mobilität sorgen sollen.

Die Fernsteuerung von Anlagenkomponenten kann dabei über eine mobile Anwendung (App) auf dem Smart Device erfolgen (siehe Bild 1), die den Bildschirminhalt der Anlagenbenutzerschnittstelle mittels Virtual Network Computing (VNC) empfängt und die Interaktion am Smart Device an die angeschlossene Komponente weiterleitet. Von Vorteil dabei ist, dass nur eine App für die Steuerung beliebiger Komponenten verwendet werden kann. Allerdings wird dabei die Nutzerschnittstelle ohne Anpassung auf dem Endgerät dargestellt, sodass beispielsweise zu kleine Steuerelemente schwer bedienbar sind. Zudem muss der vollständige Schnittstelleninhalt grafisch übertragen werden, was eine höhere Verbindungsgeschwindigkeit voraussetzt. Aus diesem Grund bieten verschiedene Hersteller spezialisierte Apps an, die für die Darstellung auf mobilen Endgeräten besser

[1] *Kim Zetter (2011): How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History, http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/.*

[2] *B. Bencsáth, G. Pék, L. Buttyán, and M. Félegyházi (2011): Duqu: A Stuxnet-like malware found in the wild, http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf*

[3] *Kim Zetter (2012): Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers, http://www.wired.com/threatlevel/2012/05/flame/all/*

[4] *BMBF, Industrie 4.0, http://www.bmbf.de/de/19955.php*

optimiert sind und eigene Schnittstellen beinhalten, die dann aber meist nur innerhalb des Komponentensortiments des Herstellers eingesetzt werden können. Konzeptionell unterscheiden sich diese Ansätze bezüglich der IT-Sicherheit für das Produktionsumfeld jedoch nicht. Solange die Verbindung zur Anlage besteht, können Befehle gesendet werden und Daten ausgelesen werden.

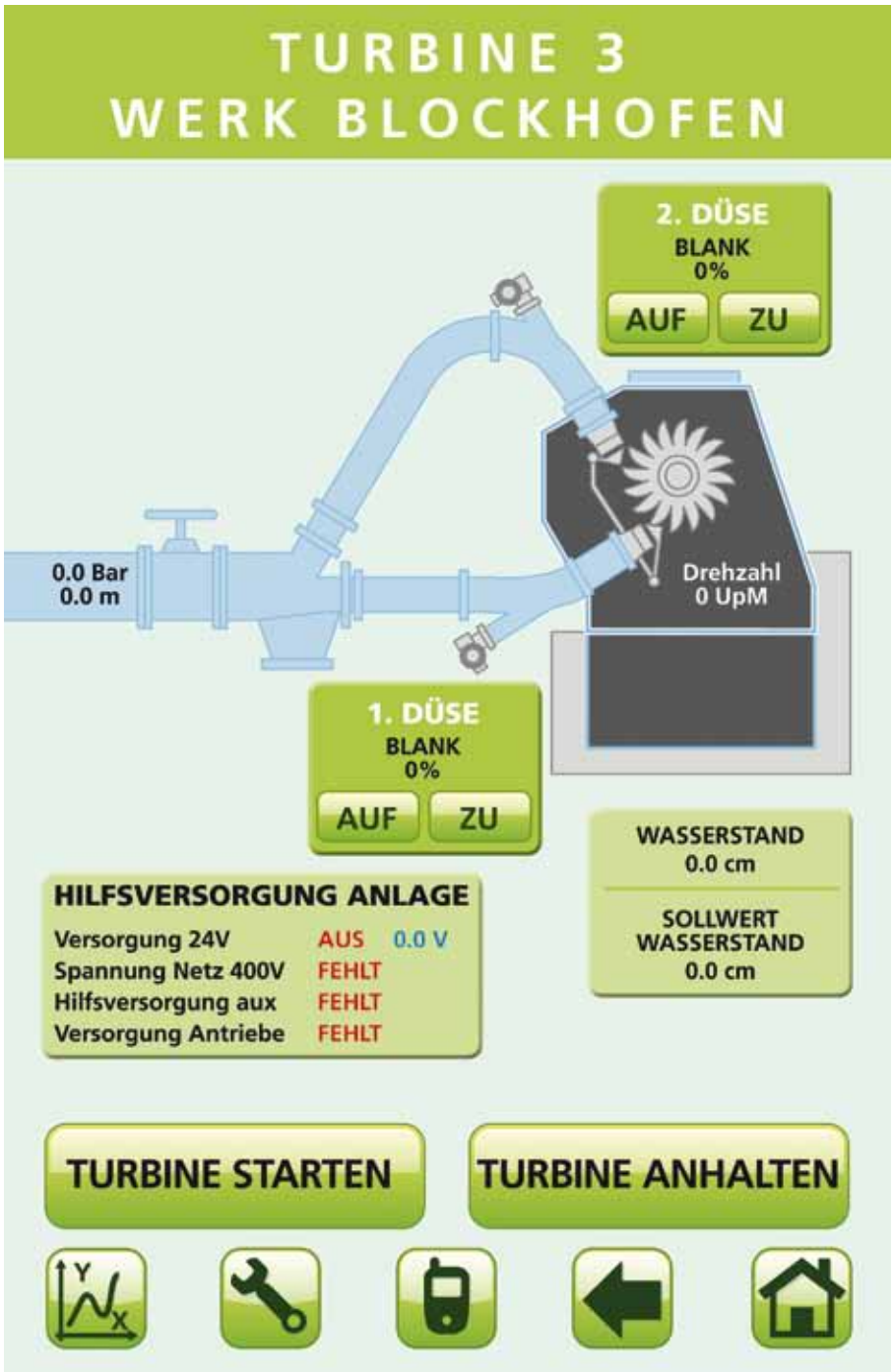

Bild 1: Visualisierung einer Turbinensteuerung zur Fernsteuerung

Wenn Unternehmen bewusst die Entscheidung treffen, Prozesse durch neue Endgeräte örtlich unabhängiger zu gestalten, ist die IT-Abteilung der zentrale Anlaufpunkt. Wenn Mitarbeiter aber unaufgefordert ihre privaten Geräte über die darauf installierte Software für betriebliche Zwecke einsetzen, bleibt die betriebliche Kontrolle außen vor. Somit erhalten nicht nur Consumer-Geräte Einzug ins Unternehmen, sondern auch Apps, deren Vertrauenswürdigkeit und Unbedenklichkeit kaum oder nie geprüft wurde.

Unternehmensschutz für Smart Devices

Kleine mobile Geräte gelangen oft unbemerkt ins Unternehmen. Sie haben damit bereits eine erste Sicherheitshürde überwunden. Dabei geht es keineswegs nur um Smartphones und Tablets: Inzwischen wird häufig auch vor präparierten USB-Sticks gewarnt[5], die nach dem Einstecken ohne weiteres Zutun Unternehmensnetzwerk und Anlagen angreifen können. Auch andere USB-Geräte wie beispielsweise präparierte Computermäuse[6], USB-Tassenwärmer und auch Smartphones als USB-Gerät können auf ähnliche Weise manipuliert sein.

Neben diesem physischen Aspekt gibt es jedoch weitere Punkte, die eine Neubetrachtung der IT-Sicherheit im Produktionsumfeld beim Einsatz von Smart Devices erforderlich machen. Zu beginnen ist dabei zunächst bei den allgemeinen Schutzzielen. Bei der Steuerung von Produktionsanlagen sind Schutzziele häufig danach zu bewerten, in welchem Umfeld sich die zu schützende Komponente befindet. Im Büroumfeld muss sicherlich hauptsächlich die Vertraulichkeit von Produktions-Know-how und dessen Integrität gewährleistet werden, um Piraterie und Produktionsfehler zu vermeiden. In den eigentlichen Steuerungsnetzwerken ist hingegen die Verfügbarkeit der Produktionssysteme maßgeblich, wenn Systemausfälle finanzielle Schäden verursachen. Aus diesem Grund ist es zunächst wichtig zu betrachten, wie und in welchem Bereich Smartphones und Tablets im Produktionsumfeld genutzt werden. Aktuell finden diese einfach und schnell Anwendung für vielfältige Tätigkeiten, in denen ursprünglich unterschiedliche Geräte eingesetzt wurden. Die mobilen Alleskönner werden so zur zentralen Plattform, die sich zwischen verschiedenen internen und ex-

[5] *BSI (2011), BSI-Lagebericht IT-Sicherheit 2011, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011_nbf.pdf*

[6] *Heise-Online (2012), Angriff der Computer-Maus, http://heise.de/-1269684*

ternen Netzen bewegt und in den Arbeitsabläufen unterschiedliche Rollen einnimmt. Mit den Aufgaben wächst jedoch auch die Angriffsfläche. Aus diesem Grund müssen die Angriffspunkte identifiziert werden und es ist genau festzustellen, wie und womit sich die Smart Devices im Unternehmen verbinden.

Zudem ist auch zu betrachten, wie die Datenanzeige und Anlagensteuerung auf den Geräten durchgeführt wird. Zum einen müssen die genutzten Apps vertrauenswürdig sein, zum anderen ist auf eine entsprechende Qualität der Sicherheitsfunktionalität zu achten.

Plattformsicherheit der Smart Devices

Zur Nutzung von Smart Devices mit Unternehmensdaten benötigen die Geräte Zugriff auf Unternehmensdienste wie beispielsweise E-Mail, Dokumentenverwaltung oder Wartungsschnittstellen. Entsprechende Kennwörter muss der Nutzer bei der Anmeldung am Dienst dem Gerät indirekt anvertrauen, unabhängig davon, ob diese im Gerät gespeichert werden oder nicht. Daher besteht eine Vertrauensbeziehung zwischen den Geräten und den genutzten Diensten. Es existieren in diesem Fall keine Barrieren, da Nutzer und Gerät legitimiert sind. Daraus entstehen bereits erste Angriffsmöglichkeiten auf die Geräteplattformen und damit das Unternehmensnetzwerk. Zum einen lassen sich über ein angegriffenes Smart Device Daten auslesen, zum anderen kann aber auch die Steuerung von Anlagen übernommen werden, wenn der legitime Nutzer, dessen Smart Device kompromittiert wurde, die Berechtigung dazu hat.

Zum Ausnutzen potenzieller Schwachstellen in Smart Devices muss der Angreifer zunächst mit dem Gerät in Kontakt kommen, entweder physisch (beispielsweise durch Diebstahl) oder aus der Entfernung durch manipulierte Daten. Letzteres kann exemplarisch durch den Besuch einer präparierten Webseite zum Ausnutzen von Fehlern im Browser erfolgen oder durch den Empfang von manipulierten Dateianhängen via E-Mail, SMS oder anderen Kommunikationsdiensten. Einen Überblick über weitere potenzielle Angriffsvektoren und Beispiele für deren Ausnutzbarkeit beschreibt auch der Artikel „Geht Ihr Smartphone fremd?“ [7].

Unabhängig von potenziellen technischen Schwächen sind für die Risikobetrachtung jedoch auch folgende Aspekte relevant:

Anforderungen: Viele der Plattformen sind für Consumer-Geräte konzipiert. Das macht sie meist einfach zu bedienen, kann aber auch dazu führen, dass Unternehmensanforderungen hinsichtlich der Sicherheitsqualität nicht im Vordergrund stehen.

Consumer-Betriebssysteme: Aufgrund der hohen Verbreitung von Consumer-Geräten und dem häufigen Wunsch der Nutzer darin bestehende Sicherheitseinschränkungen der Geräte zu Gunsten von mehr Funktionalität zu umgehen (sogenannter Jailbreak beziehungsweise Rooting), stehen Angreifern bereits freie Werkzeuge zur Verfügung und es ist wenig spezialisiertes Know-how notwendig, um in diese Geräte einzudringen und damit gezielt Unternehmen anzugreifen. Dies kann auch für angepasste Industriegeräte gelten, die mit Consumer-Betriebssystemen arbeiten, wenn diese zwar besser an die physischen Anforderungen angepasst sind, darüber hinaus aber keine Härtung des Bootloaders und des Betriebssystems erfolgt ist.

Angriffswahrscheinlichkeit: Angriffe, die originär auf Endnutzer im Massenmarkt ausgerichtet sind, können beim Einsatz von Consumer Smart Devices auch auf Unternehmen Einfluss nehmen, auch wenn diese nicht zielgerichtet im Fokus des Angreifers waren.

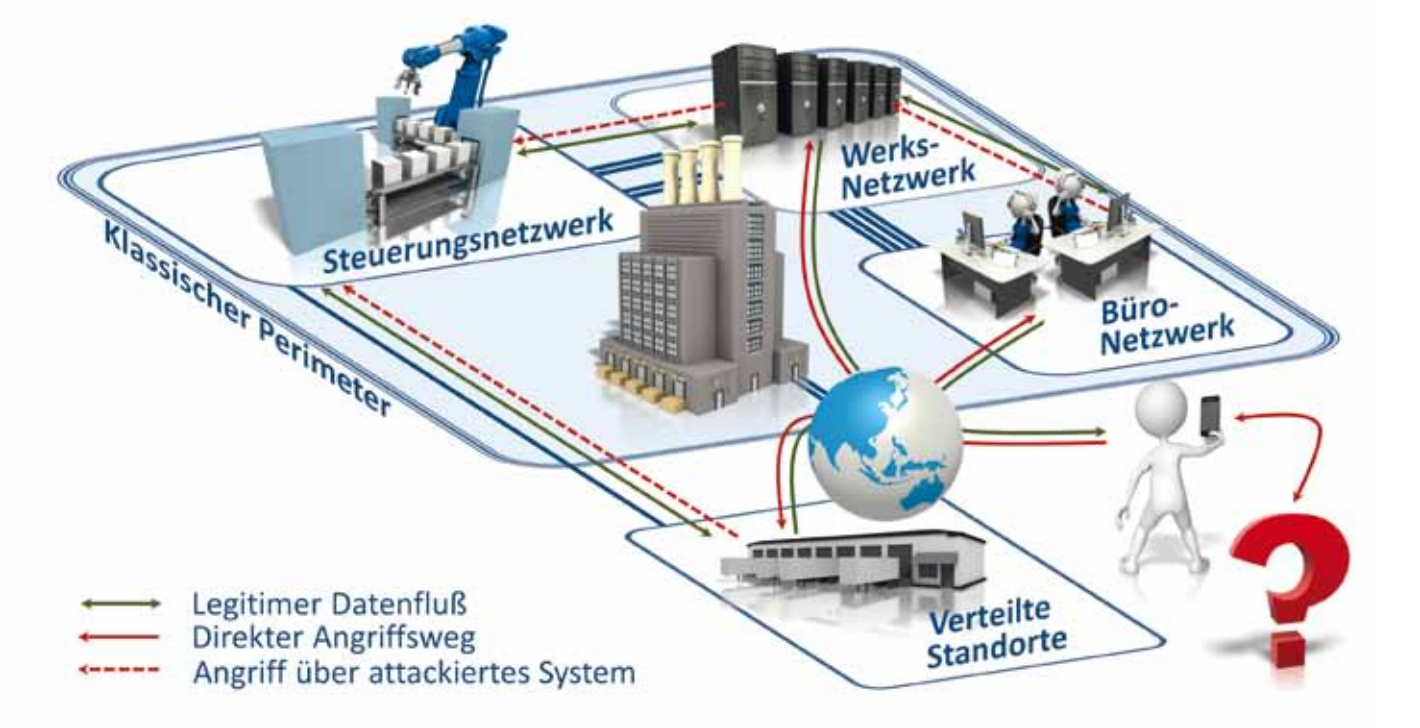

Bild 2: Zugriffspfade von Smart Devices und resultierende Angriffswege bei kompromittierten Geräten

Erreichbarkeit: Kabellose Geräte bieten für Angreifer generell den Vorteil, aus der Entfernung unbemerkt Kontakt zu möglichen Schwachstellen im Gerät aufnehmen zu können. Aber auch die Nutzung von öffentlichen ungesicherten oder nicht vertrauenswürdigen Netzwerken (WiFi-Hotspots) erhöht die Chancen für Angreifer, kommunizierte Inhalte mitzulesen oder in die Verbindung einzugreifen.

Nutzungsumfeld: Da Smart Devices häufig auch außerhalb des Unternehmens genutzt werden, besteht auch ein höheres Risiko, dass Daten vom Display einsehbar sind. Zudem sind auf Geräten mit Touchscreen die Eingabemasken für Passwörter durch die visuelle Bestätigung der Bildschirmtastaturen leicht mitzulesen (sogenanntes Shoulder Surfing), was auch automatisiert erfolgen kann[8].

Netzwerksicherheit

Erst durch den Zugriff auf Daten und Dienste eines Unternehmens wird die Nutzung von Smart Devices sinnvoll. Dazu muss von der Netzwerkseite ein Zugriff erlaubt werden, der jedoch auch ohne Smart Device durch andere genutzt werden kann. Selbst wenn für den Zugriff auf die Daten eine Nutzerauthentifizierung erforderlich ist, besteht die Gefahr, dass der bereitstellende Server auf Netzwerkebene angreifbar ist. Firewalls mit Deep-Packet-Inspection können zwar sicherstellen, dass nur freigegebene Dienste angesprochen werden, aber auch diese sind unter Umständen angreifbar (beispielsweise per Brute-Force-Angriff, bei dem alternierend für m verschiedene Accounts n Passwörter durchprobiert werden). Eine Absicherung per Virtual Private Network-Lösung (VPN), die eine Anmeldung am Netzwerk erfordert und häufig für die Notebook-Anbindung Verwendung findet, reduziert das Angriffspotenzial weiter, führt bei instabilen Mobilfunkverbindungen jedoch zu schlechter Benutzbarkeit. Zudem sind die Anmeldedaten für den VPN-Zugang bei Smart Devices wegen der beschränkten Eingabemöglichkeiten in der Regel auf den Smart Devices gespeichert und diese Ablage ist teilweise schlecht geschützt (für Apple iOS siehe beispielsweise [9]).

Da die Netzwerk-Topologie üblicherweise eine komplexere Vernetzung mit Systemen Dritter aufweist (Support, Kooperationspartner, Tochterunternehmen, Außenstellen usw.) ist ferner zu berücksichtigen, dass modifizierte oder infizierte Smart Devices in diesen Netzwerken eingesetzt werden beziehungsweise für Angriffe genutzt werden können. Daher sind bei der Risikobewertung und Schutzbedarfsfeststellung nicht nur die direkten Übergabepunkte zum Internet beziehungsweise Intranet zu berücksichtigen, sondern auch die mittelbaren Schnittstellen. Auch die spontane Installation und der Betrieb von Wi-Fi-Hotspots und Wi-Fi-Tethering am Smart Device können unkontrollierte Netzwerkbrücken eröffnen, über die sich Verbindungen zu ungeschützten Steuerungsnetzwerken aufbauen lassen. Daher ist es sinnvoll, auch diese potenziellen Brücken zumindest organisatorisch durch Regeln zu beschränken und regelmäßig deren Einhaltung zu kontrollieren.

Neben der direkten Vernetzung auf TCP/IP-Ebene und dem Industrial Ethernet ist gerade im Produktionsumfeld die Verknüpfung mit weiteren Protokollen wie beispielsweise Feldbussystemen und EIA-485 zu betrachten, die zunächst keine IT-Sicherheitsfunktionalität im Sinne von Netzwerkschutzmaßnahmen aufweisen. Werden Daten dieser Protokolle mittels TCP transportiert (beispielsweise bei CAN-Ethernet Gateways), sind auch Angriffe über infizierte Smart Devices mit Zugriff auf das transportierende Netz möglich, wenn keine zusätzlichen kryptographischen Schutzmechanismen (Authentifikation, Verschlüsselung) wie in IPSec in den Netzwerken zum Einsatz kommen.

Anwendungssicherheit

Neben dem allgemeinen Schutz von Smart Device-Plattform und -Netzwerk ist auch die Sicherheitsqualität der mobilen Anwendungen von wesentlicher Relevanz. Auch wenn Apps auf dem Smart Device durch die etablierten Sandbox-Konzepte der Smart Device Plattformen von den Daten anderer Apps weitestgehend getrennt sind, müssen Apps zur direkten Steuerung oder mit direktem Zugriff auf relevante Daten von Produktionsanlagen dennoch hochwertig und vertrauenswürdig sein. So sind neben potenziellen Malware-Aktivitäten aller Apps (Entwenden von Daten oder unautorisierte Aktivierung von Sensoren wie Kamera und Mikrofon) auch die Schutzmechanismen der Unternehmens-Apps zu berücksichtigen. Zudem ist es wichtig, dass die Apps den Anforderungen entsprechend konzeptionell abgesichert und korrekt implementiert sind. Dabei gilt es im Allgemeinen folgendes zu hinterfragen:

Kommunikation: Wird die Kommunikation zur Steuerungsanlage anforderungsgemäß geschützt und wird dabei beispielsweise auch die Authentizität der Gegenstelle korrekt geprüft (korrekte Zertifikatskettenprüfung bei SSL)? Hierbei treten allgemein in der Praxis häufig Schwächen auf, die von Angreifern in öffentlichen Netzen leicht zum Mitlesen oder Einschleusen von Daten ausgenutzt werden können [10].

Anwendungsdaten: Wie werden Daten auf dem Gerät abgelegt und wie sind diese bei Geräteverlust geschützt? Dabei sind auch temporäre Daten zu berücksichtigen, die vom Betriebssystem teilweise ohne Kenntnis des Entwicklers und Nutzers erstellt werden.

Credentials (Anmeldedaten): Welche Passwörter und Zertifikate werden auf dem Gerät gespeichert und wie sind diese geschützt? Die bei der Nutzung eingegebenen Credentials stellen ein wesentliches Angriffsziel dar, da mit diesen ein fortwährender Zugriff auf aktuelle Daten und das Auslösen von Aktionen möglich ist.

7 *J. Heider, R. El Khayari (2012): Geht Ihr Smartphone Fremd?, DuD 3/2012, http://sit4.me/geht-smartphone-fremd*

8 *Heise-Online (2012), iPhone als Passwortspion, http://heise.de/-1280011*

9 *J. Heider, R. El Khayari (2012): iOS Keychain FAQ, http://sit4.me/ios-keychain-faq*

10 *Heise-Online (2012), Verschlüsselung bei vielen Android-Apps mangelhaft, http://heise.de/-1732351*

Ressourcennutzung: Welche Sensoren (Kamera, Mikrofon usw.) und Daten anderer Apps (beispielsweise Adressbuch, Kalender und Drittanbieter-Daten) werden von der App verwendet? Die Ressourcennutzung kann dabei Richtlinien zum Vertraulichkeitsschutz verletzen. Ebenso ist es möglich, dass Berechtigungen der App von anderen Apps missbraucht werden (auch bekannt als Confused Deputy Problem).
Kryptographie: Welche kryptografischen Funktionen werden genutzt und werden diese korrekt für die Schutzziele eingesetzt? Zudem ist zu hinterfragen, ob die Funktionen aus bewährten Standardbibliotheken oder Eigenimplementierungen verwendet werden. Gerade in diesem Bereich kommt es immer wieder zu Implementierungsfehlern, die gravierende Auswirkungen auf die Gesamtsicherheit der App haben.
Backend: Wie ist die Interaktion mit der Logik des Backends hinsichtlich Berechtigungsmanagement gesichert und wie ist das Backend gegen Angriffe gehärtet? Zum einen können Angriffe durch manipulierte Apps erfolgen, die auf das Umgehen von Einschränkungen der Berechtigung abzielen, zum anderen durch manipulierte Daten, die dem Angreifer durch Fehler in der Verarbeitung im Backend weiteren Zugang verschaffen (zum Beispiel durch Injection Attacks und Buffer Overflows).

Diese Kriterien sind individuell für alle eingesetzten Apps auf den Smart Device Plattformen zu betrachten. Da jedoch bei Apps aus den App-Märkten häufig keine detaillierten Informationen zu diesen Fragestellungen vorliegen, bleibt nur das Durchführen von Sicherheitstests, um die Sicherheitsgüte von Apps zu ermitteln. Auch beim Einsatz von Entwicklungen, die für ein Unternehmen von Dritten erzeugt wurden, ist es sinnvoll, die gestellten Sicherheitsanforderungen in der Praxis von unabhängiger Seite verifizieren zu lassen. Besonders effizient lassen sich solche Prüfungen anhand des Quellcodes durchführen (Whitebox Test). Wenn dieser nicht vorliegt, können aber auch wichtige Aussagen aus der ausführbaren App extrahiert werden (Blackbox Text), wozu am Fraunhofer SIT neue effiziente Verfahren entwickelt wurden.

Empfehlungen

Smart Devices sollten nur nach sorgfältig geplanter Sicherung und Kontrolle zum Einsatz kommen. Eine Nutzung mit den Standardkonfigurationen der Geräte ist zu vermeiden, da diese in der Regel zu viel unsichere Funktionalität erlauben und ungeeignete Einstellungen für Unternehmen enthalten. Das BSI rät zu generellen Schutzmaßnahmen wie beispielsweise den Einsatz einer zentralen Geräteverwaltung, die Nutzung von Verschlüsselung und Umsetzung sicherer Passwortrichtlinien für Smart Devices[11]. Allgemein kann aber der Einsatz von Smart Devices ohne Gerätekennwort (oder mit weniger als fünf alphanumerischen Stellen) im Produktionsumfeld nicht empfohlen werden.

Durch die wechselnden Rollen von Smart Devices und der daraus resultierenden Angriffsmöglichkeit von innen bieten Firewalls zur Netzsegmentierung nur noch einen (jedoch wichtigen) Basisschutz. Eine wesentliche Zusatzmaßnahme ist, dass sich nicht nur Benutzer am Netzwerk authentifizieren, sondern – im Sinne von Network Access Control (NAC) – zuerst auch die Smart Devices. Gegenwärtig ist das nur durch zusätzliche Software auf den Geräten im Zusammenspiel mit Komponenten im Netzwerk möglich. So können Geräte, auf deren Schutzniveau und Vertrauenswürdigkeit vom Unternehmen kein Einfluss genommen werden kann oder die eine unsichere Software (Apps und/oder Smart Device Betriebssystem) aufweisen, vom Netzwerk ausgeschlossen werden. Durch eine Kombination mit Mobile Device Management Lösungen (MDM) lassen sich die nunmehr durchweg bekannten Geräte zentral konfigurieren – ein weiteres Element zur Sicherung der Infrastruktur. Die Sicherheit an den eigentlichen Fertigungs- und Steueranlagen profitiert davon zwar nicht direkt, dennoch lässt sich das Risiko von Wirtsumgebungen in den vorgelagerten Netzwerken wirkungsvoll reduzieren.

Apps für den Zugriff auf Produktionssysteme oder für die Nutzung von Unternehmensdaten sind bei der Sicherung ebenfalls zu berücksichtigen. Je nachdem, wie diese die Schutzmöglichkeiten der Smart Device Plattform nutzen, wie zusätzliche Maßnahmen implementiert sind und welche Schwachstellen darin enthalten sind, beeinflusst dies entscheidend das Verwundbarkeitsniveau. Daher sind Sicherheitsanalysen der Apps, die im Unternehmen zum Einsatz kommen, eine weitere wichtige Maßnahme, zusätzlich zu den App-Tests der Märkte.

Last not least müssen auch die Nutzer der Geräte entsprechend für die Gefahren sensibilisiert und den richtigen Umgang geschult werden. Die besten technischen Maßnahmen lassen sich problemlos aushebeln, wenn sie nicht mit einem adäquaten Verhalten einhergehen.

Fazit

Wie in anderen Bereichen bieten Smart Devices auch im Produktionsumfeld vielfältige Anwendungsmöglichkeiten. Gerade dort ist jedoch die Integration in Arbeitsprozesse genau zu prüfen, da es für einen sicheren Einsatz einer entsprechenden Einbeziehung der Netzinfrastruktur in das Schutzkonzept bedarf und für Konfiguration und Betrieb entsprechendes Know-how der Sicherheitsimplikationen der Plattformen notwendig ist. Mit bestehenden Lösungen zur Verwaltung von Smart Devices, einer den Schutzzielen angemessenen Beschränkung der Funktionalität und dem Stärken des Wissens der Mitarbeiter über Angriffsmethoden kann das verbleibende Risiko deutlich reduziert werden. Für kritische Bereiche ist aber selbst mit diesen Ansätzen derzeitig von einem Einsatz abzuraten. Diese Bereiche sollten so abgesichert werden, dass generell kein unkontrollierter Zugriff über Smart Devices und andere portable Geräte und Medien möglich ist. ■

Dr. Jens Heider,
Abteilungsleiter Testlabor Mobile Sicherheit am Fraunhofer-Institut für Sichere Informationstechnologie (SIT) in Darmstadt

[11] *BSI (2011), Überblickspapier Smartphones, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_Smartphone_pdf.pdf*