Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: HERSTELLER

Sichere Passwörter in Embedded Devices

Verhinderung von Schwachstellen durch Standardpasswörter und festcodierte Zugangsdaten

Embedded Devices kommen mittlerweile in sämtlichen Bereichen des täglichen Lebens zum Einsatz. Anwendungsbereiche sind unter anderem industrielle Steuerungskomponenten (z. B. Speicher-programmierbare Steuerungen), Netzwerktechnik (Router und Switche), Bürogeräte (Drucker, Scanner, Kopierer), Unterhaltungselektronik (Set-Top Boxen) sowie Automotive oder Flugzeugbau.

Hierbei handelt es sich häufig um netzwerkfähige Komponenten, in denen dieselben Dienste implementiert werden, die auch bei Serversystemen zu finden sind (HTTP(S), FTP, TELNET, SNMP, etc.). Der Zugriff auf diese Standarddienste ist in der Regel über einen Passwortschutz gesichert.

Embedded Devices werden meist mit vorkonfigurierten Standardpasswörtern ausgeliefert. Diese Standardpasswörter lassen sich anhand der oftmals online verfügbaren Produktdokumentation oder über Onlineforen einfach in Erfahrung bringen. Die Benutzernamen sind über diese Quellen ebenso leicht zu eruieren oder sogar direkt aus der Webschnittstelle herauslesbar (z. B. wenn die existierenden Benutzernamen in Form einer Dropdownliste dargestellt werden). Da eine Änderung der vordefinierten Passwörter/Benutzernamen im Rahmen der Integration und Inbetriebnahme der Geräte häufig nicht stattfindet, kann ein Angreifer somit (Voll-)zugriff auf ein solches Gerät erlangen, ohne Schadsoftware oder dedizierte Tools einsetzen zu müssen.

Noch kritischer als solche voreingestellten, aber änderbaren Standardpasswörter sind Passwörter, die fest in einem Gerät implementiert sind. Hierbei kann es sich zum einem um festcodierte, dokumentierte Benutzerpasswörter handeln, aber auch um – zumeist undokumentierte – Hintertüren (Backdoors), über die ein Zugriff auf das Gerät möglich ist. Letztere stammen teilweise aus der Entwicklungsphase und wurden vor der Auslieferung des fertigen Produktes nicht entfernt. Mitunter sind diese Hintertüren auch absichtlich vom Hersteller eingerichtet worden, um im Problemfall einen Wartungszugang zu haben. Sie dürfen aber keinesfalls als Produktfeature angesehen werden. Bei Industriesteuerungen können Hintertüren nämlich beispielsweise dazu missbraucht werden, um unberechtigten Zugriff auf eine Steuerung zu erlangen, eine Änderung der Konfiguration vorzunehmen, Schadsoftware im Betriebssystem aufzuspielen oder um das Steuerprogramm herunterzuladen bzw. ein manipuliertes Steuerprogramm zu installieren.

Die Häufigkeit solcher Schwachstellen spiegelt sich unter anderem in der Vielzahl von Produktwarnungen (Advisories) wieder, welche das US-amerikanische ICS-CERT fortlaufend veröffentlicht. Dass auch andere Gerätearten betroffen sind, zeigt die jüngste Arbeit der IT-Sicherheitsexperten Billy Rios und Terry McCorkle. In etwa 300 medizinischen Geräten von 40 verschiedenen Herstellern konnten sie gravierende Schwachstellen im Bereich der Passwortsicherheit entdecken. Ein anderer unbekannter Sicherheitsexperte hatte 2012 über 420.000 Embedded Devices genutzt, um diese zu einem Botnetz zusammenzuschließen und so eine "Vermessung" des Internets vorzunehmen ("Internet Census"). Für den Zugriff auf diese 420.000 Embedded Devices wurden ausschließlich Standardpasswörter genutzt.

1 Empfehlungen für Hersteller

Hersteller von Embedded Devices, in denen ein Passwortschutz zur Anwendung kommt, sollten folgende Lösungsmöglichkeiten in Betracht ziehen:

- Hinweis in der Dokumentation – möglichst an herausragender Stelle – dass ein Standardpasswort gesetzt ist und dieses dringend geändert werden muss.
- Hinweis in der Administrationsoberfläche, dass ein Standardpasswort gesetzt ist.
- Erzwingen der Änderung bei Installation bzw. initialer Konfiguration.
- Auslieferung erfolgt bereits mit individuellem Passwort (z. B. abgeleitet von Seriennummer, MAC-Adresse, ...), welches nach Factory Reset wieder gesetzt wird.
- Verzicht auf Hintertüren und festcodierte Zugangsdaten.

Zusätzlich zu den genannten Umsetzungsmöglichkeiten gibt es weitere flankierende Maßnahmen, wie z. B. in der Dokumentation aufgeführte Anforderungsempfehlungen an sichere Passwörter (Komplexität, maximale Gültigkeit) oder die technische Durchsetzung solcher Password Policies. Hinweise zu komplexen Passwörtern finden Sie z. B. im „Leitfaden Informationssicherheit“[1] (Seite 56 ff) des BSI.

Auch ist sicherzustellen, dass Passwörter nicht durch den Zugriff auf Konfigurations- oder Logdateien oder über andere Mechanismen, wie SNMP, ausgelesen werden können.

Weiterhin sollten Passwörter immer unter Verwendung hinreichend sicherer kryptografischer Mechanismen gespeichert und übertragen werden. Beispielsweise bietet es sich an, Password-Based Key Derivation Function 2 (PBKDF2), bcrypt (auf Basis des Kryptoalgorithmus Blowfish) o. ä. zu verwenden. Zumindest sollte aber ein Salted Hash genutzt werden, bei dem als Eingabe in eine Hashfunktion neben dem Passwort ein Zufallswert eingeht, um Angriffe mit vorberechneten Daten zu erschweren. Verfahren wie MD5 oder SHA-1 (ohne Salt) sind als unsicher zu bewerten. Von einer Verwendung ist daher abzuraten.

Bei der Authentisierung mittels Passwörtern verbleiben natürlich gewisse Restrisiken, wie z. B. Angriffe durch systematisches Ausprobieren (Brute Force) oder Wörterbuchangriffe. Neben Mindestanforderungen an die Komplexität von Passwörtern (Password Policies) sollten daher auch fehlgeschlagene Login-Versuche protokolliert werden. Beim Überschreiten eines zu definierenden Schwellwertes von fehlgeschlagenen Anmeldeversuchen sollten zudem Meldungen über SNMP oder andere Mechanismen initiiert werden. Sofern keine Safety-Aspekte dagegen sprechen, kann nach Fehleingaben auch eine temporäre Sperrung des Zugangs erfolgen. Zur Verhinderung automatisierter Angriffe ist es bereits ausreichend, den Zugang beispielsweise nach 5 Fehlversuchen für eine Minute zu sperren.

Zumindest perspektivisch ist die Nutzung anderer Authentisierungsmechanismen (z. B. Multifactor) in Betracht zu ziehen.

1 https://www.bsi.bund.de/dok/6604834

2 Empfehlungen für Integratoren / Errichter

Im Zuge der Integration sollten für alle Benutzerkennungen individuelle und hinreichend komplexe Passwörter gewählt werden.

Die an den Kunden übergebene Dokumentation sollte an hervorgehobener Stelle diejenigen Anforderungen enthalten, welche für ein hinreichendes Sicherheitsniveau bei der Authentisierung mittels Passwörtern einzuhalten sind (z. B. Passwortkomplexität oder feingranulare Nutzerverwaltung).

Um die Angriffsfläche zu minimieren, empfiehlt es sich, nicht benötigte Dienste und Accounts zu deaktivieren. Bei der Integration eines Geräts oder einer Maschine in eine Netzinfrastruktur sollte eine Segmentierung gewählt werden, bei der kritische IT-Systeme, also z. B. solche, bei denen die Authentisierung mittels Passwort erfolgt, möglichst nicht direkt über das Internet zugänglich sind. Ist eine Erreichbarkeit über das Internet erforderlich, so sollten diese Systeme über eine VPN-Lösung abgesichert werden.

3 Empfehlungen für Betreiber

Auf Betreiberseite ist eine Verwaltung der verwendeten IT-Systeme (Asset Management) zu etablieren. Dies ermöglicht u. a. die zeitnahe Prüfung der Betroffenheit durch Schwachstellen. In Kombination mit einem Sicherheitsmanagement können die Risiken von Schwachstellen bewertet und geeignete Gegenmaßnahmen gefunden werden.

Empfehlungen der Hersteller und Integratoren zur Komplexität von Passwörtern, deren regelmäßige Änderung und dem weiteren Umgang mit diesen sind zwingend zu beachten.

Es sollten möglichst flankierende Maßnahmen umgesetzt werden – entweder integriert in die zu schützenden Geräte oder durch ergänzende Komponenten. Hierzu gehört beispielsweise die Nutzung von MAC- oder IP-Filtermechanismen oder die Detektion von Brute Force Angriffen.

Sofern aus betrieblicher Sicht möglich, sollten sowohl die Geräte selbst als auch ergänzende Sicherheitskomponenten (Firewalls, Antivirensoftware, etc.) zeitnah mit Security Patches versorgt werden. Hierfür sind sowohl die Hinweise der Hersteller als auch die der jeweiligen CERTs zu beachten.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an info@cyber-allianz.de gesendet werden.