Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IN DER PRODUKTION

Industrial Control System Security

Innentäter

In der Vergangenheit sind Industrielle Steuerungen mangels Vernetzung fast nur durch Angriffe vor Ort bedroht gewesen. Mit dem Aufkommen der neuen Cyber-Bedrohungen ist diese Innentäterproblematik aber nicht obsolet. Vielmehr ist sie durch immer weiter gehende Arbeitsteilung noch relevanter geworden. Im Fokus stehen dabei jedoch nicht nur Angriffe gegen die industriellen Anlagen eines Betreibers selbst. Auch die gesamte Lieferkette (Supply Chain) ist zu berücksichtigen, denn alle beteiligten Dienstleister und Geschäftspartner bilden als potenzielle Innentäter jeweils einen zusätzlichen Angriffsvektor.

Potenzielle Innentäter sind sämtliche Personen mit (privilegiertem) Zugriff auf bzw. Zutritt zu IT-Komponenten, IT-Diensten, Installationen, Dokumenten oder sonstigen ggf. kritischen Informationen und Geräten. Insbesondere sind hierbei folgende Personenkreise zu nennen:

- Personen mit unmittelbarem physischen Zugriff auf Steuerungsanlagen (z. B. Bediener, Ingenieure)
- Personen mit privilegierten Rechten (z. B. Administratoren)
- Personen mit indirektem Zugang, z. B. auch zum Office-Netz oder zu Verwaltungsgebäuden
- Mitarbeiter von Dienstleistern (z. B. Wartung oder Softwareentwicklung), Lieferanten, etc.

Innentäter stellen ein Risiko dar, das naturgemäß niemals vollständig ausgeschlossen werden kann. Daher ist es wichtig, dass geeignete Vorkehrungen getroffen werden, um die Gefahren beherrschbar zu machen. Allerdings dürfen sowohl die eigenen Mitarbeiter als auch Externe nicht den Eindruck bekommen, unter Generalverdacht zu stehen.

Dieses Dokument gibt eine Reihe von Empfehlungen zum Umgang mit der Bedrohung durch Innentäter. Eine gemeinsame Betrachtung mit anderen Themen, wie Fernwirken und Fernwartung, ist dabei durchaus sinnvoll. Jedoch werden solche Themen in diesem Dokument nicht im Schwerpunkt behandelt, da hierzu separate BSI-Veröffentlichungen zur Cyber-Sicherheit erarbeitet werden.

1 Mögliche Angriffe

Bei der Betrachtung von Innentätern sind insbesondere die folgenden Angriffsarten zu berücksichtigen:

- Verlust bzw. Diebstahl von Informationen (Data Leakage) durch Zugriffsmöglichkeiten auf Fileserver, Datenträger oder IT-Systeme. Neben

elektronischen Dokumenten sind natürlich auch physische Dokumente zu berücksichtigen. Motivation für Datendiebstähle können sowohl Industriespionage als auch Whistleblowing (Bekanntmachung von Missständen; vgl. Wikileaks) sein.

- Social Engineering – insbesondere zur Vorbereitung von Folgeangriffen, z. B. durch Ermittlung von Ansprechpartnern, Prozessbeschreibungen, IT-Architekturen, Rezepturen oder Steuerprogrammen. Personen mit Zutritt zu bestimmten Bereichen könnten zudem Mitarbeiter zu Aktionen, wie beispielsweise Installation von Software über externe Wechseldatenträger, Konfigurationsänderungen an IT-Systemen oder Weitergabe kryptografischer Schlüssel, verleiten, um Angriffspfade zu eröffnen.
- Sabotage – insbesondere begründet durch politische oder wirtschaftliche Interessen – ist eine mögliche Angriffsform, für die eine erhöhte Bedrohung durch Innentäter besteht. Hierzu gehört beispielsweise die Manipulation von Steuerungskomponenten oder das Einschleppen von Schad- oder Spionagesoftware. Solche Schadsoftware kann zudem (unbeabsichtigt) durch fahrlässiges Verhalten eingeschleppt werden.

2 Allgemeine organisatorische Sicherheitsmaßnahmen

Die folgenden organisatorischen Maßnahmen (Security Controls) sind geeignet, um der Bedrohung durch Innentäter vorzubeugen. Diese Maßnahmen sollten im Sicherheitsmanagement und in den zu definierenden Sicherheitskonzepten berücksichtigt werden.

- Inventarisierung: Eine elementare Maßnahme ist das Erfassen sämtlicher potenzieller Innentäter sowie deren Privilegien. Dies beinhaltet die Dokumentation sämtlicher Zugriffsmöglichkeiten bzw. Accounts für Benutzer, Administratoren und Externe, wobei Funktions-/Gruppen-Accounts besonders kritisch zu hinterfragen sind. Gerade bei externen Mitarbeitern sollten geltende Service Level Agreements und sonstige vereinbarte Regelungen (z. B. Security Policies) erfasst werden. Die Umsetzung einer solchen Erfassung erfolgt als fortlaufender Prozess bzw. als Teil des Security-Managements. Sie sollte in Kombination mit IT Asset Management erfolgen, also der Verwaltung der Netzwerke, Systeme, Anwendungen, Dokumente (z. B. Fileserver) sowie des Personals in einer Gesamtbetrachtung. Dabei sollten auch Aspekte wie Fernwirken und Fernwartung behandelt werden. Die Erfassung kann z. B. mittels Systemanalysen, Interviews und Vor-Ort-Begehungen erfolgen.
- Festschreibung von Policies für unterschiedliche Gruppen von Mitarbeitern: Dies umfasst z. B. Verhaltensregeln für die Verwendung von Wechseldatenträgern oder Regelungen zum Umgang mit und der Weitergabe von Dokumenten. Mitarbeiter sind gemäß dieser Policies zu sensibilisieren und zu schulen. Auch externe Mitarbeiter sollten zur Einhaltung der Policies des beauftragenden Unternehmens verpflichtet und entsprechend geschult bzw. instruiert werden. Insbesondere bei international agierenden bzw. verteilten Unternehmen sollten dabei lokale – z. B. geopolitische – Gegebenheiten berücksichtigt werden.
- Identitäts- und Berechtigungsmanagement: Es erfolgt der unmittelbare Widerruf von Berechtigungen (IT & physisch) bei Wegfall der Notwendigkeit. Hierzu gehört auch das Ändern der Passwörter von betroffenen Gruppen-/Funktions-Accounts. Besonders für Neueinstellungen sowie aus dem Unternehmen ausscheidende Mitarbeiter und Mitarbeiter, welche die Rolle innerhalb des Unternehmens wechseln („Starters, Leavers & Movers“), sind geeignete Prozesse zu definieren, die einen sicheren und konsistenten Zustand gewährleisten. Hierzu gehört beispielsweise die Rückgabe von IT-Geräten, Authentisierungstoken oder Mitarbeiterausweisen. Das eingesetzte Personal wird – insbesondere in den besonders kritischen Bereichen – einer regelmäßigen Prüfung unterzogen (Background Check). Mitarbeiter sollten zudem auf die Pflichten und Verantwortlichkeiten sowie die Folgen von Zuwiderhandlungen hingewiesen werden.

- Etablierung eines Change Managements: Ad hoc Änderungen („auf Zuruf“) an Systemen sind explizit auszuschließen. Insbesondere sicherheitskritische Prozesse sollten das Prinzip der Rollenteilung (Separation of Duties) sowie das Vier-Augen-Prinzip berücksichtigen.
- Durchsetzung einer strikten Zutrittskontrolle: Der Zutritt zum Unternehmen allgemein sowie zu unterschiedlichen Bereichen sollte reglementiert werden. Mitarbeiter- bzw. Besucherausweise mit unterschiedlichen Berechtigungen sollten deutlich voneinander unterschieden werden können (z. B. farbliche Kennzeichnung).
- Verwaltung von Schlüsseln: Schlüssel für die Aktivierung von Fernwartungszugängen mittels Schlüsselschalter werden an zentraler Stelle unter Verschluss gehalten und nur bei Bedarf herausgegeben. Hierzu ist ein Schlüsselbuch zu führen, in dem vermerkt wird, wann und wem welcher Schlüssel herausgegeben wurde bzw. wann dieser zurückgegeben wurde.
- Whistleblower: Insbesondere eigenen Mitarbeitern sollte intern eine Möglichkeit zur Verfügung stehen, um vertraulich auf Missstände hinweisen zu können.

3 Ergänzende technische Maßnahmen

Ergänzend sind u. a. die folgenden technischen Maßnahmen geeignet, um in der Summe einen möglichst umfassenden Schutz gegen Innentäter zu etablieren. Dabei ist anzustreben, diese Maßnahmen möglichst zentral zu bündeln – beispielsweise in Form eines Security Information & Event Management (SIEM) sowie eines Identity & Access Managements (IAM / IDM).

- Die Verwendung hinreichend sicherer Authentisierungsmechanismen (z. B. Token) ermöglicht ein hohes Maß an Sicherheit. Es sollten möglichst ausschließlich individuelle Accounts mit hinreichender Authentisierung (z. B. Multi-factor) verwendet werden.
- Beim Einsatz von Zugangskontrollsystemen unter Verwendung digitaler Ausweise besteht die Möglichkeit, die Einhaltung der festgelegten Zutrittsbeschränkungen durch technische Maßnahmen zu prüfen. Solche digitalen Ausweise können zugleich als Token zur Anmeldung an IT-Systemen genutzt werden (Synergieeffekte). Zutrittskontrollen können zudem beispielsweise mittels Videoüberwachung im Rahmen der rechtlichen Möglichkeiten flankiert werden.
- Bei Steuerungen (z. B. Speicher-programmierbare Steuerungen, SPS) sollten ggf. vorhandene Möglichkeiten genutzt werden, damit ein Bedienereingriff mit einer Authentisierung oder nach dem Vier-Augen-Prinzip abgesichert werden muss.
- Die Beschränkung der Zugriffsmöglichkeiten auf Ressourcen mittels technischer Sicherheitskomponenten (Firewalls, uni-direktionale Gateways) gewährleistet, dass erforderliche Daten aus anderen Bereichen (z. B. Office-Netz) bezogen werden können, ohne dass gleichzeitig kritische Möglichkeiten zur Einflussnahme auf IT-Systeme resultieren.
- In IT-Systemen verfügbare Mechanismen für Timeouts von Nutzersitzungen sowie passwortgeschützte Bildschirmschoner sind nach Möglichkeit zu verwenden.
- Umsetzung von Virenschutz auf Netzwerk- und ggf. Hostebene für Server, Workstations und Terminals: Je nach Szenario kann alternativ auch Application Whitelisting zur Beschränkung der zulässigen Applikationen und Prozesse umgesetzt werden. (Wechsel-)Datenträger von Externen bzw. aus anderen Unternehmensbereichen (z. B. Office-Netz) werden vor dem Einsatz im Produktionsnetz einer Virenprüfung unterzogen, beispielsweise durch Einsatz spezieller Terminals (Wechseldatenträgerschleuse).

- Einsatz von Device Control Lösungen, um die Verwendung von unzulässigen Wechseldatenträgern und USB-Geräten zu verhindern.

Neben Maßnahmen zur Verhinderung von Sicherheitsvorfällen durch Innentäter sind insbesondere solche Maßnahmen wichtig, welche solche Vorfälle aufdecken können.

- Möglichkeiten zur Detektion von Manipulationen und Kompromittierungen bietet ein automatisiertes Monitoring von IT-Systemen sowie deren Konfigurationen und Logdateien. Beispielsweise können CPU- und Speicher-Auslastung, Anzahl/Profil der Prozesse, Anzahl und Art der Netzverbindungen, fehlgeschlagene Authentisierungsversuche, etablierte Netzwerkrouten, Datenvolumen oder über die Konfigurationsdaten gebildete Hashwerte fortlaufend erfasst und überwacht werden.
- Es sollte eine automatische Detektion neuer IT-Systeme und Netzwerkkomponenten im Netz erfolgen. Dies gilt sowohl für drahtgebundene als auch für drahtlose Netze (z. B. WLAN Access Point).

4 Sicherheitsmaßnahmen bei externen Mitarbeitern (Fremdfirmen)

- Fremdfirmen benennen einen Ansprechpartner für IT-Sicherheitsfragen.
- Sicherheitsvorfälle seitens der Fremdfirmen sind unverzüglich an den festgelegten Ansprechpartner im beauftragenden Unternehmen zu melden.
- Juristische Regelungen zur Geheimhaltung (Non-disclosure Agreements, NDA) sind unverzichtbar.
- Eine Unterbeauftragung sowie die Nutzung von Outsourcing oder externen Clouddiensten bedürfen der expliziten schriftlichen Erlaubnis durch das beauftragende Unternehmen.
- Fremdfirmen müssen ein Identitätsmanagement und ein Berechtigungskonzept für die eigene IT etabliert haben.
- Auf der Webseite des beauftragenden Unternehmens sollte eine Möglichkeit existieren, damit sich Servicetechniker zum Besuch anmelden können und dort die Vorgaben und Policies zur Kenntnis nehmen können/müssen.
- Es erfolgt ein Security-Check externer Service-Notebooks mit anschließender Ausstellung eines Besucher-Zertifikats, um damit Netzwerkzugriff zu bekommen.
- Vertrauliche Daten werden durch Externe ausschließlich verschlüsselt übertragen und gespeichert.
- Von externen Unternehmen wird eine Zertifizierung gemäß etablierter Standards, wie IT-Grundschutz oder ISO 27000, gefordert.
- In besonders kritischen Einsatzbereichen erhalten Fremdfirmen ausschließlich unter bestimmten Bedingungen Zutritt, z. B. unter Begleitung und nur während der Tagesschicht.
- Zugänge zu internen IT-Systemen werden mit einer zeitlichen Beschränkung eingerichtet.
- Zugriffe auf und Änderungen an kritischen IT-Systemen unterliegen einem hinreichend sicheren und detaillierten Logging-Mechanismus.
- Right to Audit: Das beauftragende Unternehmen ist berechtigt, die Einhaltung der Sicherheitsvorgaben zu prüfen bzw. durch Dritte prüfen zu lassen.