Cyber-Security

Suzhou, 2017

IT-Sicherheit ist überaus wichtig für kritische Infrastrukturen wie Strom- und Wasserversorgungssysteme, Transportsysteme und Anlagensteuerungen, die mithilfe von IT-Systemen betrieben werden. Die zunehmende Offenheit dieser Infrastrukturen bietet eine immer größere Angriffsfläche, und Industriespionage und Cyber-Attacken stellen eine wachsende Bedrohung dar. Damit steigen auch die Sicherheitsanforderungen für Siemens-Produkte und –Lösungen kontinuierlich, die vom Markt, den Kunden sowie von gesetzlichen Bestimmungen diktiert werden.

Experten von Siemens' Corporate Technology (CT) sind Spezialisten für rechtzeitige Präventionsverfahren und systematische Abwehr. Insbesondere die Integration von IT-Sicherheit in einem frühen Entwicklungsstadium kann Mehrwert schaffen und Verzögerungen bei der Markteinführung von Produkten verhindern.

Angriffe und Industriespionage

- Konservativen Analysen des deutschen Branchenverbands BITKOM zufolge (Studie von April 2015) beläuft sich der Schaden, der der deutschen Wirtschaft durch digitale Industriespionage, Sabotage und Datendiebstahl entsteht, auf jährlich rund 51 Mrd. Euro.
- Zahllose Hackergruppen verüben Industriespionage, wobei sie normalerweise über Internet-Browser und E-Mail-Systeme angreifen.
- Angriffe über Social Engineering sind auf dem Vormarsch. Das gilt ebenso für Attacken, die unmittelbar über das Internet der Dinge (Internet of Things, IoT) und ungeschützte IoT-Geräte erfolgen.
- Siemens erhält jeden Tag 3,5 bis 4 Millionen E-Mails, von denen nahezu 50 Prozent Spam-Mails sind oder sogar infizierte Links enthalten.
- Siemens betreibt weltweit mehrere Cyber Defense Center (CDC) – zu seinem eigenen Schutz und zum Schutz der Kunden. So werden beispielsweise in einem CDC jeden Monat rund 1.000 Alarmmeldungen registriert. Rund 30 davon sind besonders kritische Vorfälle, die dann zusammen mit dem Cyber Emergency Response Team (CERT) von Siemens bearbeitet werden.

SIEMENS
Ingenuity for life

Zuständigkeit für Sicherheit

Seit Oktober dieses Jahres sind die Zuständigkeiten für IT-Sicherheit bei Siemens auf zwei Einheiten verteilt.

- Corporate Technology ist zuständig für die unternehmensweite Planung und Steuerung der Informationssicherheit sowie der Sicherheit von Produkten und Lösungen.
- Global Services Information Technology ist zuständig für die Implementierung von Informationssicherheit.

Security by design

Die Fachleute von Corporate Technology integrieren Sicherheit systematisch in Prozesse und Produkte nach dem so genannten „Security by Design"-Ansatz. Das bedeutet, dass Sicherheit in den Produktlebenszyklus eingebaut wird, von der Entwicklung bis zum Betrieb.

Die technischen Aspekte sind:

- Sichere Kommunikation (Authentifizierung und Verschlüsselung etc.)
- Zugangskontrolle
- Systematisches Hardening, integriertes Patch-Management und Sicherheitstests sowie
- Benutzerfreundlichkeit, damit Benutzer auch in der Lage sind, die Sicherheitsvorkehrungen und -einrichtungen richtig anzuwenden.

Interne Hacker und „golden nuggets"

- Unsere CT-Experten überwachen die Systeme von Siemens und erkennen Angriffe für gewöhnlich rechtzeitig oder verhindern sie mit Schutzmaßnahmen von vornherein. Ein Beispiel ist Ransomware, bei der ein Hacker einen Rechner von außen lahmlegt und den Code für die Aktivierung des Rechners erst nach Zahlung eines Lösegelds herausgibt. Dank der eingerichteten Sicherheitsvorkehrungen ist Siemens bislang durch solche Angriffe kaum Schaden entstanden.
- So genannte „golden nuggets", eine Bezeichnung für strategisch wichtige und unternehmenskritische Daten, deren Verlust für Siemens ein großer Schaden bedeuten würde, erhalten eine Sonderklassifizierung und sind jeweils durch ein umfassendes Sicherheitskonzept geschützt.

- Aufgrund des anhaltenden Trends, Anwendungen und Systeme ins Internet zu verlegen, gibt es auch einen Bedarf an cloudfähigen Sicherheitssystemen. Die Experten von CT arbeiten auf diesem Gebiet zum Beispiel an der Identitätsüberwachung von Benutzern und Zugriffsrechten.
- Um Sicherheitslücken zu entdecken, bevor ein echter Cyber-Pirat zuschlägt, beschäftigt CT ein eigenes Team von Hackern, die versuchen, in Siemens-Systeme einzudringen.

Umgang mit identifizierten Schwachstellen in Siemens-Produkten

- Wenn in Produkten von Siemens oder in Fremdkomponenten, die in Siemens-Produkte eingebaut sind, Schwachstellen erkannt werden, sorgen bewährte Prozesse dafür, dass diese so schnell wie möglich beseitigt werden und Kunden so genannte Advisories oder Patches erhalten.

Datenanalyse für Cyber-Security

Die Datenanalyse spielt eine Schlüsselrolle für die Datensicherheit in allen möglichen Anwendungsfällen, zum Beispiel beim Erkennen von Angriffen und der Schadensbewertung. Aufgrund des zunehmenden Umfangs sicherheitsrelevanter Daten und der Komplexität von Cyber-Angriffen wird es immer wichtiger, dass IT-Sicherheitsexperten leistungsfähige Analysemethoden zur Verfügung haben. Bei Corporate Technology arbeiten IT-Sicherheitsexperten und Fachleute für Datenanalyse in diesem Bereich zusammen. Sie generieren verwertbare Informationen und Sicherheitswissen aus Daten und ermöglichen auf diese Weise den Business Units, neue und bessere Services und Lösungen zu verfolgen.