Industrie 4.0 und Cyber-Risiken

Geschäftsrisiken im digitalen Zeitalter

Verfasst von Phil Kibler, Leiter Cyber RiskConsulting, AIG

Im vergangenen Jahr sind viele prominente Unternehmen mit Industrie 4.0 Applikationen (Internet of Things, IoT)[1] Opfer von Denial-of-Service-Angriffen (DoS) geworden. Im Oktober 2016 ist der große DNS-Provider Dyn Opfer eines massiven DoS-Angriffs geworden. Internetnutzer an der US-Ostküste konnten auf eine Reihe von beliebten Webseiten wie Twitter, Amazon, PayPal, Spotify, Reddit, Netflix und andere nicht mehr zugreifen.

Einen Monat zuvor, im September 2016, wurde Brian Krebs (ein bekannter Journalist für Cyber-Sicherheit) mit seiner Webseite Opfer eines DoS-Angriffsversuchs, der in der Historie von Cyber-Angriffen als einer der massivsten gilt. Die Analyse des Botnet, das an diesem Angriff beteiligt war, ergab, dass insbesondere IoT-Geräte betroffen waren. Der Angreifer loggte sich mit Standardzugangsdaten ein und weitete sich dann auf andere angeschlossene Geräte aus. Nachdem das Botnet Zugriff auf über 400.000 IoT-Geräte hatte, startete es seinen Angriff und war in der Lage, einen Denial-of-Service-Angriff in dieser Dimension zu starten.

Bei einem Denial-of-Service-Angriff versucht ein Angreifer die rechtmäßigen Nutzer daran zu hindern, auf Informationen oder Dienste zuzugreifen. Wenn Angreifer Ihren Computer und dessen Netzwerkverbindung oder die Computer und das Netzwerk Ihres Standorts ins Visier nehmen, kann er Sie problemlos daran hindern, auf E-Mails, Webseiten, Accounts (Online-Banking usw.) oder andere Geräte, die mit dem betroffenen Computer verbunden sind, zuzugreifen.[2]

Warum ist ein solcher Angriff möglich und wodurch wird eine Netzwerkumgebung anfällig für Angriffe? Viele Unternehmen halten ihre IoT-Geräte nach der Installation nicht kontinuierlich auf dem aktuellen Stand. Darüber hinaus sind einige IoT-Geräte nicht von sich aus in der Lage, Patches zu empfangen, damit sich ihre Sicherheitseinstellungen regelmäßig aktualisieren.

Es gibt mittlerweile konkurrierende Botnets, die IoT-Geräte angreifen. AIG ist daher überzeugt, dass es in naher Zukunft sehr wahrscheinlich ist, dass es weitere große Angriffe geben wird. Es gibt mindestens ein weiteres IoT-Botnet, das etwa eine Million Geräte beeinträchtigt hat![3] Unternehmen müssen daher sicherstellen, dass ihre IoT-Geräte korrekt installiert sind und regelmäßig durch Software-Updates aktualisiert werden, um die Gefährdung eines Angriffs zu verringern.

Was können Unternehmen tun?

- Erstellen Sie ein Verzeichnis aller IoT-Geräte, damit Ihnen das Ausmaß der Gefährdung klar ist.
- Wenn die IoT-Plattform über eine Standard-ID und ein Standard-Passwort verfügt, ändern Sie diese. Angreifer kennen die Plattformen und deren Standardeinstellungen.
- Wenn Sie das Passwort ändern, wählen Sie eines, das als sicher gilt und Folgendes beinhaltet:
  - Mindestens acht Zeichen;
  - Mindestens eine Zahl, einen Buchstaben und einen Großbuchstaben und
  - falls erlaubt, mindestens ein Satzzeichen.
- Passwörter sollten regelmäßig geändert werden und komplex bleiben, d. h. kein Ort, kein Name und keine anderen leicht zu erratenden Benutzerinformationen.
- Prüfen Sie rechtzeitig und regelmäßig, ob Patches verfügbar sind, und/oder stimmen Sie zu, dass Updates und Patches automatisch installiert werden, wenn die IoT-Plattform dies erlaubt.
- Deaktivieren Sie die Remoteverwaltung und andere überflüssigen Funktionen.
- Erlauben Sie keinen ungefilterten Zugriff auf das Gerät vom Internet aus; gewähren Sie nur Verbindungen von der Whitelist (vertrauenswürdige Verbindungen) Zugriff über IP-Filterung oder andere Sicherheitskontrollen.
- Erlauben Sie kein Universal Plug and Play auf IoT-Geräten.
- Verwenden Sie, wenn möglich, sichere Protokolle, wie HTTPS und SSH zur Gerätekommunikation.
- Integrieren Sie IoT-Geräte in regelmäßige Programme zum Schwachstellen-Management.

Wenn Ihr Unternehmen oder Ihre Mitarbeiter Opfer einer Cyber-Attacke werden, steht mehr auf dem Spiel als Daten. In einem sich schnell verändernden Umfeld kann eine Cyber-Verletzung oder -Attacke zu Sachschäden, längerer Betriebsunterbrechung oder Schäden für die Kunden führen. Aus diesem Grund bietet AIG seinen Kunden proaktive Risikodienstleistungen, umfassenden Versicherungsschutz sowie seit Langem bestehende Teams für Datenschutzverletzungen und Schadenregulierung, die Ihnen helfen, bei Cyber-Gefahren einen Vorsprung zu gewinnen. Weitere Informationen finden Sie unter www.aig.com/cyberedge.

1 IoT-Geräte umfassen DVR- und IP-Kameras, Kühlschränke, intelligente Zähler, Telefone, Kaffeemaschinen, Thermostate, Router, Kabelmodems, Drucker, Fernseher, E-Zigaretten usw.

2 https://www.us-cert.gov/ncas/tips/ST04-015

3 http://thehackernews.com/2016/10/linux-irc-iot-botnet.html

DEL00001527 FEB17