Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
Neidenburger Str. 43
D-45877 Gelsenkirchen
Tel.: 0209 9596 746

Pressemitteilung

Alte IT-Systeme sind ein enormes Sicherheitsrisiko in der Industrie

Gelsenkirchen, 30.05.2012 – Das Institut für Internet-Sicherheit – if(is) der Westfälischen Hochschule in Gelsenkirchen bietet Kooperationspartnern ab sofort Spitzenexpertise im Bereich der industriellen IT-Sicherheit an.

Im industriellen Bereich hat die rasante Entwicklung der Informationstechnologie in den letzten Jahren eine weitreichende Vernetzung industrieller Komponenten auch über das Internet erfahren. Die Anbindung von industriellen Komponenten an das Internet bringt IT-Sicherheitsrisiken, die einen sehr hohen Schaden haben können.
Durch lange Systemlaufzeiten von 24 Stunden an 365 Tagen im Jahr und mehr wird die zugehörige IT-Infrastruktur lange nicht verändert.

Die Bedrohungen sind real

Ein grundsätzliches Problem im industriellen Umfeld resultiert aus den verhältnismäßig langen Technologie-Life-Cycles.
„Viele Unternehmen verwenden noch IT-Systeme in ihren Produktionsstätten, die seit zehn Jahren nicht mehr verändert wurden. Jeder Angreifer entdeckt hier ohne weiteres hunderte von Schwachstellen, die er für erfolgreiche Angriffe nutzen kann“, so Prof. Norbert Pohlmann, Leiter des Instituts für Internet-Sicherheit. Pohlmann weiter: „Wenn Angreifern solche Angriffsflächen geboten werden, dann werden sie diese auch nutzen, was zu sehr hohen Schäden führen wird.“ Ein erster zielgerichteter Angriff in der Branche fand in Form der Stuxnet Malware auf ein bestimmtes System zur Überwachung und Steuerung technischer Prozesse (SCADA-System) der Firma Siemens statt.

Strukturelle Ursachen

Die IT-Angriffsflächen im industriellen Umfeld sind strukturell bedingt, da in diesen Unternehmen das Hauptaugenmerk auf die Prozesse gerichtet ist. Es wird das reibungslose Funktionieren von Automatisierungs-, Prozess-, Leit- und Steuerungstechnik im Sinne der Safety (Unversehrtheit des Menschen und der Maschinen) angestrebt.
Die einmal laufenden Systeme und die hierfür entwickelte Software werden ohne besonderen Anlass nicht mehr verändert „Never change a running system“, was um Jahre veraltete Systeme bedeutet.

Auswirkungen der Schwachstellen

Industrielle Umgebungen finden sich in vielen der für die Gesellschaft sehr wichtigen Kritischen Infrastrukturen (KRITIS) und unterliegen vor dem Hintergrund der gezielt ausgebeuteten Schwachstellen einem hohen Risikopotential. Ein Ausfall kann nicht absehbare volkswirtschaftliche Schäden und gesundheitliche Gefährdungen für Menschen

E-Mail: GonzalezRobles@internet-sicherheit.de
Internet: www.internet-sicherheit.de

bedeuten. Die Folgen eines erfolgreichen Angriffs auf die IT von beispielsweise Stromnetzen, Chemieanlagen, der Wasserversorgung, des Gesundheitswesens oder des Transportwesens wären für sich allein betrachtet verheerend, könnten sich aber nach dem Dominoeffekt zu einer Katastrophe entwickeln.

Allein der Ausfall eines Stromnetzes könnte Produktionsstätten, Verkehrs-, Transportsysteme, Informationstechnik, Telekommunikation und weitere Bereiche der Gesellschaft stark beeinflussen, wenn nicht sogar außer Betrieb setzen.
Ein erfolgreicher Angriff auf eine Chemieanlage könnte eine schleichende vorerst nicht bemerkte Kontamination von Mensch und Umwelt bis hin zu einer immensen Explosion zur Folge haben.

Abschaltung der Risiken

Die Behebung der Schwachstellen zur Abschaltung des Risikos durch deren Ausbeutung gestaltet sich mehrstufig. In einem ersten Schritt müssen Sicherheitsbetrachtungen allen Entwicklungsschritten voran gehen. Die Softwareentwicklung im industriellen Umfeld muss grundlegend adaptiert werden, sodass von Anfang an sowohl prozess- wie vernetzungsbedingte IT-Sicherheits-Risiken Berücksichtigung finden, damit nicht erst am Ende der Entwicklung die IT-Sicherheit der bestehenden Lösung nur aufgesetzt wird, anstatt sie zu integrieren.
In einem weiteren Schritt muss auch im industriellen Umfeld die Betrachtung der IT-Sicherheit als dynamischer fortwährender Prozess erfolgen, sodass regelmäßig und bei Bedarf außerplanmäßig erkannte Sicherheitslücken durch Updates (Aktualisierungen) unmittelbar geschlossen werden können.

Das Institut für Internet-Sicherheit - if(is) bietet eine gemeinschaftliche Vorgehensweise mit den industriellen Partnern an, sodass das besondere industrielle Branchenwissen mit dem besonderen Augenmerk auf Safety und die langjährige Expertise des Instituts im IT-Sicherheitsumfeld eine Lösung ermöglichen, die dem Safety und „IT-Security“ Anspruch gerecht wird.

Im Forschungsbereich „Security for Smart Car, Smart Grid, Smart Traffic und Smart Home“ widmet sich das Institut für Internet-Sicherheit – if(is) auch der Fragestellung der Safety-gerechten Betrachtung der Bedürfnisse der industriellen IT-Sicherheit.

Weitere Informationen zu diesem Forschungsbereich finden Sie unter:
https://www.internet-sicherheit.de/smart-security

Autor und Pressekontakt:

Dipl.-Ing. Antonio González Robles
Wissenschaftlicher Mitarbeiter
Institut für Internet-Sicherheit – if(is)
GonzalezRobles@internet-sicherheit.de

Westfälische Hochschule Gelsenkirchen
Neidenburger Str. 43
D-45877 Gelsenkirchen
Tel.: 0209 9596 746