Zielgerichtete Attacken auf Industrieunternehmen nehmen um mehr als ein Drittel zu

Kaspersky-Prognose: Zunahme spezieller Malware gegen industrielle Automationssysteme

Moskau/Ingolstadt, 8. Januar 2018

Jedes vierte (28 Prozent) Industrieunternehmen war in jüngster Zeit von einem Cyberangriff betroffen. Zielgerichtete Attacken nahmen dabei um mehr als ein Drittel zu, wie aus einer Studie von Kaspersky Lab hervorgeht [1]. Da die Nachfrage im Jahr 2017 nach Zero-Day-Exploits für industrielle Kontrollsysteme auf dem Schwarzmarkt signifikant anstieg, gehen die ICS CERT Experten von Kaspersky Lab davon aus, dass im Jahr 2018 spezifische Malware auftauchen wird, die es auf Schwachstellen industrieller Automationskomponenten abgesehen hat [2].

Aufgrund der zunehmenden Komplexität und Anzahl der Angriffe im Industriesektor wären die Folgen katastrophal, wenn Cybersicherheitsprobleme ignoriert würden. 28 Prozent der von Kaspersky Lab befragten Industrieunternehmen waren in der jüngeren Vergangenheit mit einem zielgerichteten Angriff konfrontiert [3] – das sind acht Prozentpunkte mehr gegenüber dem Vorjahr (20 Prozent). Die deutliche Zunahme solcher Attacken weist darauf hin, dass es Cyberkriminelle vermehrt auf Unternehmen im Industriesektor abgesehen haben und daher entsprechende Malware entwickeln werden, die es speziell auf industrielle Automationskomponenten abgesehen hat.

Die Hälfte (48 Prozent) der Industrieunternehmen gibt an, dass sie keinen ausreichenden Einblick in mögliche Cyberbedrohungen hat, mit denen das eigene Unternehmen konfrontiert sein könnte. Angesichts der mangelnden Einsicht in das Netzwerk stimmen 87 Prozent der Industrieunternehmen zu, dass die registrierten Sicherheitsvorfälle komplex gewesen seien. Mit zunehmender Komplexität der Cyberattacken benötigen Industrieunternehmen im Durchschnitt mehrere Tage (34 Prozent) bis hin zu mehreren Wochen (20 Prozent), um einen Sicherheitsvorfall zu entdecken.

(Un)-Sicherheitsfaktor Mensch

Die Mehrheit (62 Prozent) der Mitarbeiter in Industrieunternehmen ist überzeugt, dass der Einsatz einer entsprechenden Sicherheitslösung nötig ist; rund die Hälfte (49 Prozent) beschuldigt jedoch die eigenen Mitarbeiter, IT-Sicherheitsrichtlinien nicht ordnungsgemäß zu

befolgen. Neben dem Einsatz einer Sicherheitslösung [4] sind daher Schulungen und Mitarbeitertrainings [5] für einen umfassenden Schutz in Unternehmen notwendig.

„Cyberangriffe auf industrielle Kontrollsysteme sind für viele zum unumstrittenen Hauptanliegen geworden“, so Andrey Suvorov, Head of Critical Infrastructure Protection Business Development bei Kaspersky Lab. „Die gute Nachricht ist, dass die Mehrheit der industriellen Marktteilnehmer weiß, welche Bedrohungen derzeit existieren und in naher Zukunft relevant sein werden. Daher ist es von entscheidender Bedeutung, eine komplexe Sicherheitslösung zu implementieren, die speziell für den Schutz automatisierter industrieller Umgebungen konzipiert sowie hochflexibel und entsprechend den technologischen Prozessen der jeweiligen Organisation konfiguriert ist.“

Kaspersky-Portfolio für die Industrie

Kaspersky Lab bietet für die unterschiedlichen Bedürfnisse von Industrieunternehmen mehrschichtige Schutztechnologien und -services – beispielsweise für SCADA-Server, HMIs (Human-Machine-Interface), industrielle Workstations, speicherprogrammierbare Steuerungssysteme (SPS), Netzwerkverbindungen und Mitarbeiter. Kaspersky Industrial Cybersecurity [6] ist eine ganzheitliche Lösung, die alle Phasen des adaptiven Sicherheitsmodells abdeckt – von der Vorhersage neuer Angriffsvektoren bis zum Einsatz spezialisierter Technologien für Prävention, Erkennung und Reaktion.

Weitere Informationen zu Kaspersky Industrial Cybersecurity sind unter https://www.kaspersky.de/enterprise-security/industrial zu finden.

[1] Die Studie basiert auf der „IT Security Risks Survey 2017“, die jährlich im Auftrag von Kaspersky Lab in Zusammenarbeit mit B2B International erstellt wird.

[2] https://ics-cert.kaspersky.com/reports/2017/11/30/industrial-enterprise-and-iot-security-threats-forecast-for-2018/

[3] http://newsroom.kaspersky.eu/fileadmin/user_upload/de/Downloads/PDFs/Kaspersky_Top_6_Incidents.JPG

[4] https://www.kaspersky.de/enterprise-security/industrial

[5] https://www.kaspersky.de/enterprise-security/security-awareness

[6] https://www.kaspersky.de/enterprise-security/industrial

Nützliche Links:

- Kaspersky Industrial Cybersecurity: https://www.kaspersky.de/enterprise-security/industrial
- Kaspersky Security Awareness: https://www.kaspersky.de/enterprise-security/security-awareness

Über Kaspersky Lab

Kaspersky Lab ist ein global agierendes Cybersicherheitsunternehmen, das im Jahr 2017 sein 20-jähriges Firmenjubiläum feiert. Die tiefgreifende Threat Intelligence sowie Sicherheitsexpertise von Kaspersky Lab ist Basis für Next Generation Sicherheitslösungen und -Services zum Schutz von Unternehmen, kritischen Infrastrukturen, staatlichen Einrichtungen sowie Privatanwendern weltweit. Das umfassende Sicherheitsportfolio des Unternehmens beinhaltet führenden Endpoint-Schutz sowie eine Reihe spezialisierter Sicherheitslösungen und -Services zur Verteidigung vor komplexen und aufkommenden Cyberbedrohungen. Mehr als 400 Millionen Nutzer und 270.000 Unternehmenskunden werden von den Technologien von Kaspersky Lab geschützt.

Weitere Informationen zu Kaspersky Lab finden Sie unter http://www.kaspersky.com/de/. Kurzinformationen erhalten Sie zudem über *www.twitter.com/Kaspersky_DACH und www.facebook.com/Kaspersky.Lab.DACH. Aktuelles zu Viren, Spyware, Spam sowie Informationen zu weiteren IT-Sicherheitsproblemen und -Trends sind unter https://de.securelist.com/* und auf dem Kaspersky-Blog auf *http://blog.kaspersky.de/ abrufbar.*

Redaktionskontakt:

Berkeley Kommunikation GmbH
Florian Schafroth
florian.schafroth@berkeley.global
Tel.: +49-89-7472-62-43
Fax: +49-89-7472-62-17
Landwehrstraße 61
80336 München

Kaspersky Labs GmbH
Stefan Rojacher
stefan.rojacher@kaspersky.com
Tel.: +49-841-98-189-325
Fax: +49-841-98-189-100
Despag-Straße 3
85055 Ingolstadt
