3 FRAGEN AN:

MIRKO ROSS

Der Gründer und CEO der Stuttgarter asvin GmbH spricht über weit vorausschauende Abwehrstrategien gegen Cyberattacken auf sicherheitskritische Systeme.

Glückwunsch zu 13,5 Millionen Euro von der Cyberagentur! Wofür genau ist die Fördersumme bestimmt?
Danke! Wobei wir jetzt erst die zweite von vier Stufen eines Wettbewerbsverfahrens der Cyberagentur erreicht haben. Das Auftragsvolumen umfasst 2,5 Millionen Euro für zwölf Monate. Die von Ihnen genannte Summe erhält unser Konsortium nur, wenn unsere Lösung den Evaluationen der Agentur auch in den Stufen drei und vier standhält. Das Projekt zielt darauf ab, Informationen zur Cybersecurity in Unternehmensnetzwerken sehr viel schneller als bisher auszutauschen. Außerdem geht es um die automatisierte Analyse von Cyberangriffen, um die Lehren daraus und etwaige Gegenmaßnahmen umgehend für das gesamte Netzwerk verfügbar machen zu können. An der Automatisierung geht wegen des Mangels an Fachkräften in der IT-Security kein Weg vorbei, zumal die Zahl der Angriffe weiterhin steil ansteigt – und wir es mit immer komplexerer Software in immer komplexeren Netzwerken zu tun haben.

Vernetzte Systeme brauchen über ihren Lebenszyklus hinweg Schutz. Wie lassen sich Risiken der Zukunft antizipieren?
Die Computer der ersten Mondmission hatten 145 000 Zeilen Code. In vernetzten Automobilen sind es 100 Millionen Zeilen. Rein statistisch schlummern in 1 000 Zeilen Code 0,5 bis drei unentdeckte logische Schwachstellen und Programmierfehler, die Cyberkriminelle potenziell als Einfallstore nutzen können. Risikoanalysen müssen die Komplexität und Vernetzung von Software – und damit ihre Fehlerwahrscheinlichkeit – ebenso ins Lagebild einbeziehen wie besonders gefährdete Teile des Netzwerks. Das können Abteilungen mit sensiblen Daten sein oder auch Firmen, die kritische Komponenten zuliefern oder in der Vergangenheit wiederholt Ziel von Cyberattacken waren. Hier sind jeweils gezielte Verstärkungen der Schutzmaßnahmen gefragt. Denn wegen der begrenzten Ressourcen bei zugleich zunehmenden Risiken kommt es auf eine intelligente Priorisierung der IT-Sicherheitsmaßnahmen an.

„Prävention, Detektion, Reaktion und Attribution sind nötig, um Cyberrisiken zu managen.“

Mit welchen Maßnahmen können sich Unternehmen vor den Cyberrisiken der Zukunft schützen?
Mit der Industrie 4.0 nimmt die Komplexität der Software, der Netzwerke und Beziehungsgeflechte zu. Hinter jeder Maschine einer Prozesskette steht eine eigene Lieferkette, jede Menge Software und zunehmend künstliche Intelligenz. Damit steigt nicht nur der Nutzen, sondern auch das Cyberrisiko. Um es zu managen, gibt es vier Handlungsfelder: erstens Prävention in Form der erwähnten Risikoanalyse sowie automatisierter, KI-basierter und umgehend ausgetauschter Angriffsanalysen. Im Sinne der Früherkennung ist zweitens engmaschige Detektion gefragt; oft werden Netzwerke schon Monate vor dem Angriff korrumpiert. Drittens ist im Ernstfall eine verhältnismäßige Reaktion gefragt: Produktion und Geschäftsbetrieb sollten nur als Ultima Ratio gestoppt werden. Und viertens ist Attribution gefragt. Denn ob es um simple Erpressung, Industriespionage oder eine staatlich gedeckte Attacke geht, hat großen Einfluss auf die Abwehrstrategie.

SECURITY BY DESIGN

Die zweitägige Weiterbildung des Maschinenbau-Instituts am 24./25.10.2023 in Karlsruhe vermittelt anhand der IEC 62443, wie Industrial Security von Beginn an mitgedacht werden kann.

Informationen
go.vdma.org/pvmb7

Illustration: Ryze Digital (Vorlage: asvin)