Beim Thema Cybersicherheit ist einiges in Bewegung, nicht zuletzt durch den Krieg in der Ukraine und durch den Konflikt im Nahen Osten. Das sagt asvin-Manager Gerhard Steininger im exklusiven Kreis beim Vortrag der Transformations-Lounge von TraFoNetz im tec21 in Nagold. ©Foto: Robin Daniel Frommer

Experte warnt Unternehmen vor offenen Flanken in der IT-Sicherheit

Die jüngste Transformations-Lounge von TraFoNetz fand im Technologiezentrum „tec21“ in Nagold statt. Im Fokus der Veranstaltung stand ein kompakter Impulsvortrag von Gerhard Steininger, Diplom-Physiker und Manager für Sales & Business Development und Vice President (VP) bei der asvin GmbH in Stuttgart. In exklusivem Rahmen ging der Referent intensiv auf die Analyse und Bewertung von Cyber-Risiken (und auf neue Methoden der Cyber-Security) ein.

Von Robin Daniel Frommer | 07.05.2024

„Asvin ist ein kleines Start-up-Unternehmen“, erläuterte Gerhard Steininger. „Es wurde vor fünf Jahren gegründet, hat rasch einige Auszeichnungen als ‚bestes Start-up‘ oder als ‚beste Lösung für Cyber-Sicherheit‘ abgeräumt und beschäftigt aktuell etwas mehr als 20 Mitarbeiter“.

IT-Security sei „ständig Thema“, macht Steininger deutlich, „da ist einiges in Bewegung, nicht zuletzt durch den Krieg in der Ukraine und durch den Konflikt im Nahen Osten“. Und er fügt hinzu: „Die Automobilindustrie ist auch ein großes Thema“. Bei Volkswagen habe man zwar versucht, einen vor ein paar Jahren erfolgten Angriff nicht nach außen zu kommunizieren, inzwischen sei jedoch bekannt, dass seinerzeit produktrelevante Daten abgefischt wurden.

TraFoNetz-Projektmanager Matthias Friedrich stellt die Leistungen des Transformationsnetzwerks Nordschwarzwald für Unternehmen und Beschäftigte in der Region vor. ©Foto: Robin Daniel Frommer

Gerhard Steiningers bildgestützte Präsentation visualisiert Cyber-Risiken in der immer komplexer werdenden Software-Industrie: „Raketentechnologie – 145.000 Programmzeilen (Lines of code, kurz LOC); zivile Luftfahrt – 12 Millionen LOC, militärische Luftfahrt – 25 Millionen LOC und Automobilindustrie – 100 Millionen LOC“. Da die Software gleichzeitig immer verwundbarer wird, zeigt er mit dem unmittelbar folgenden Chart seiner Präsentation das Gefahrenpotential von 0,5 bis 3 Fehlern pro Programmzeile auf und rechnet für moderne Fahrzeuge „50.000 bis 300.000 potentielle Fehler“ hoch.

Das sich hieraus ergebende Bedrohungsszenario sieht Steiniger zu einem Prozent bei staatlich gestützten Hackern (langfristig arbeitenden Experten, Spionen oder Geheimdiensten), „was fast vernachlässigbar“ sei. Deutlich stärker ins Gewicht fallen (mit 29 Prozent) die zielgerichteten Attacken von (nicht staatlichen) Cyber-Kriminellen, während die große Masse der Angriffe, ungefähr 70 Prozent, nicht zielspezifisch sind und von Protest-„Hacktivisten“ initiiert werden.

Was die Gefahrenabwehr anlangt, sieht Steininger bei dem Ein-Prozent-Anteil staatlich gestützter Bedrohung in erster Linie die Kosten, „da sind wir rasch im siebenstelligen Bereich“, und rät zur Konzentration „auf die potentiellen Hacker“. Außerdem sei es gerade für Mittelständler und kleinere Unternehmen wichtig zu wissen, so Steininger weiter, „mit welchen Bedrohungen sie rechnen müssen und was sie genau zu schützen haben“.

„Eine Forschergruppe in Berlin berichtete bereits über KI-generierte automatisierte Cyber-Angriffe.“
Gerhard Steininger, Manager, asvin GmbH

Patrick Walz vom TraFoNetz-Partner IHK Nordschwarzwald ist Leiter der Bereiche Technologie, Innovation und Digitalisierung. ©Foto: Robin Daniel Frommer

Das sei je nach Industriezweig, von Firma zu Firma ganz unterschiedlich. In der Automobilindustrie gehe es hauptsächlich um die „connected vehicles“ – nicht um die „alten mit dem H im Kennzeichen“. Er rechnet vor: Die konkreten Fallzahlen der Hacker-Bedrohung („threats“) wachse zuletzt kontinuierlich um jährlich 100 Prozent. Man sei bereits Ende 2021, alleine in der IT-Industrie, von 80.000 bekannten Schwachstellen („vulnerabilitys“) ausgegangen. Das habe „die IT-Abteilungen schon ziemlich beschäftigt und nervös gemacht“.

Kurz erinnert er an die 2018 in Wolfsburg kopierten Türöffnungssysteme und an den Hackerangriff auf Colonial Pipeline, Georgia, der Mitte 2021 zum vorsorglichen Abschalten der Steuersoftware des Rohrleitungsnetz‘ (und zu einer Ölkrise in den USA) geführt hatte. „Das Unternehmen konnten nicht mehr fakturieren, daher auch nicht mehr liefern – das Passwort zum Steuersystem kursierte zuvor im Dark Net“.

„Nach einer Befragung durch Cisco Systems können nur zwei Prozent der europäischen Unternehmen bei der Abwehr von Cyber-Risiken als gut aufgestellt gelten. 17 Prozent sehen sich gut gegen Hacker-Angriffe geschützt; 80 Prozent eher schlecht.“
Matthias Friedrich, TraFoNetz-Projektmanager

Zusammenfassend hält Gerhard Steininger fest: Für eine widerstandsfähige Sicherheitsstruktur („resilient security“) brauchen Unternehmen neben der Analyse und Kenntnis der Bedrohung, die Konvergenz von OT (Operational Technology) und IT sowie letztlich eine ganzheitliche Risikobetrachtung („risk by context“) samt kontinuierlicher Aktualisierung. Beispielshaft projizierte Charts seiner Graphen und Topologie basierten Analyse weisen beispielsweise für Stuttgart ein hohes Bedrohungsrisiko aus.

Zu den Kosten für den Schutz vor Cyber-Angriffen, sagte er, dass hier – auch von IT-Leitern – noch häufig starr in bestehenden Budgets gedacht wird. „Die Frage – habe ich mit meinem IT-Investment

alle Risiken abgedeckt – stelle sich kaum einem Unternehmen“. Auf Fragen aus der Runde eingehend konkretisierte er: „Ein risikoorientierter Ansatz passiert in der Regel nicht“.

Vor Gerhard Steiningers Präsentation zum Cyberrisiko-Management begrüßte Patrick Walz, (IHK Nordschwarzwald, Leiter der Bereiche Technologie, Innovation und Digitalisierung) die Teilnehmer. Matthias Friedrich, Projektmanager des Transformationsnetzwerks TraFoNetz Nordschwarzwald, stimmte auf das Thema des Abends ein und stellte die Ziele der Wirtschaftsförderung sowie Transformations- und Strategie-Tools und assoziierte Partner wie IHK und Hochschule Pforzheim vor. Außerdem ging Matthias Friedrich auf die Themen Weiterbildung, Arbeitskreise des Transformationsnetzwerks, Unternehmensbesuche und künftige Veranstaltungen sowie auf den Fachkräftemangel ein.

Transformationsnetzwerk Nordschwarzwald

Das Transformationsnetzwerk Nordschwarzwald (TraFoNetz) unter dem Dach der Wirtschaftsförderung Nordschwarzwald (WFG) ist die größte regionale Gemeinschaftsinitiative zur kostenfreien Unterstützung der Automotive-Unternehmen und ihrer Beschäftigten im Nordschwarzwald. Gefördert wird sie vom Bundesministerium für Wirtschaft und Klimaschutz. Ziel ist es, die Transformation im Automobilbereich erfolgreich zu meistern und damit den Standort Nordschwarzwald und die Arbeitsplätze zu sichern.

TraFoNetz-Partner sind unter anderem die Arbeitsagentur Nagold-Pforzheim, die Hochschule Pforzheim, die AgenturQ mit Südwestmetall und IG Metall, die IHK Nordschwarzwald, die Handwerkskammern Karlsruhe und Reutlingen, e-mobil BW, IAB Institut für Arbeitsmarkt- und Berufsforschung sowie Steinbeis InnoBW, wvib Wirtschaftsverband und weitere.

www.trafonetz.de

Medien-Kontakt TraFoNetz: Gerd.Lache@nordschwarzwald.de | 01577 3302229