Foto: Rawpixel.com - stock.adobe.com

Cyberangriffe sind auch in den grundsätzlich den kritischen Infrastrukturen (Kritis) zuzurechnenden Sparten Transport und Verkehr ein immer brisanteres Thema.

Mit ganzheitlicher Cyber-Security sicher ans Ziel

Im Transport- und Verkehrswesen erhöht ein ganzheitlicher Cybersecurity-Ansatz letztlich auch die Sicherheit der Passagiere.

JAKOB SCHMIDT

Cyberangriffe sind auch in den grundsätzlich den kritischen Infrastrukturen (Kritis) zuzurechnenden Sparten Transport und Verkehr ein immer brisanteres Thema. Doch wie gewährleistet man die Cybersecurity und damit im Endeffekt die Sicherheit der Gäste? Die einfache Antwort lautet: mit einem ganzheitlichen Ansatz. Das klingt – insbesondere im Englischen als „holistic cybersecurity approach" – logisch, erstrebenswert und führt schnell zu der Frage, wie man eine derart umfassende Vorgehensweise umsetzt. Wo anfangen, was beachten?

Am Anfang sollten die vorhandenen Systeme und Prozesse unter sicherheitsrelevanten Gesichtspunkten betrachtet werden, um die bereits existierenden Schutzmaßnahmen identifizieren und bewerten zu können. So lässt sich herausfinden, wo noch Bedarf besteht. Letztendlich geht es darum, alle geschäftskritischen Bereiche zu erkennen – also jene, die zwingend für die Fortführung des Betriebes notwendig sind. Manchmal ist das leicht zu evaluieren. Beim schienenbasierten Verkehr etwa sind die Steuerungen der Verkehrsleitsysteme und Weichen sicherlich als kritisch einzuschätzen, ein Flughafen ohne Flugleitsystem wird seine Kernaufgabe nicht erfüllen können. Relevant sind aber auch „nachgeordnete" Prozesse und Systeme. Man stelle sich vor, an einem größeren Flughafen oder Bahnhof fallen das Ticketingsystem, das Passagierleitsystem oder die Transportbänder und Rolltreppen längerfristig aus. Das Chaos und schlimmstenfalls der Zusammenbruch der Geschäftstätigkeit sind absehbar. Die Kritikalität der Prozesse lässt sich beispielsweise mit einer Risikoanalyse abschätzen, die entlang der Achsen Risiko und Eintrittswahrscheinlichkeit eine Einordnung ermöglicht.

Technischer Schutz reicht für ganzheitliche Cybersecurity nicht aus

Nachdem die geschäftskritischen und damit auf jeden Fall zu schützenden Prozesse bekannt sind, gilt es entsprechende Strategien und Konzepte zu erarbeiten, um Ausfällen vorzubeugen. Das beinhaltet technische Schutzmaßnahmen, angefangen bei einer sinnvollen Netzwerksegmentierung mitsamt bedarfsgerechtem Firewallkonzept, über Rollen- und Rechteverteilungen bis hin zu Systemen, die helfen das Netzwerk zu überwachen, um nur einige Beispiel zu nennen. Damit ist es aber nicht getan. Sprechen wir von informationstechnischen Systemen oder von Cybersecurity im Allgemeinen, sollte jedem klar sein, dass es einen hundertprozentigen Schutz nicht gibt. Durch entsprechende Analysen und die Einrichtung redundanter Systeme lässt sich das Ausfallrisiko durch einen kritischen Vorfall minimieren, aber es lässt sich nie ganz ausschließen.

Für den Fall der Fälle ist es empfehlenswert neben den allgemeinen Schutzkonzepten auch Notfallkonzepte parat zu haben. Doch das schönste Notfallkonzept hilft wenig, wenn es nur in der Schublade liegt. Der Ausfall kritischer Systeme und Einschränkungen durch Vorfälle setzen alle Beteiligten unter Stress. In dieser Situation erinnern sie sich nicht unbedingt an Pläne, von denen sie einmal gehört haben sollten. Erst durch regelmäßige Übungen bauen sich Automatismen auf, die im Notfall abgerufen werden können und durch die Mitarbeitende wissen, was zu tun und wer zu informieren ist, um den Normalbetrieb wiederherzustellen.

Schutz und Usability im Konzept ausbalancieren

Auch wenn der Worst Case nicht eintritt, ist es sinnvoll, Mitarbeitende darin zu schulen, Cyberattacken zu erkennen, sie vertraut zu machen mit allgegenwärtigen Angriffsmustern, wie Social Engineering, Phishing und Konsorten, und ihnen zu erklären, warum Security-Prozesse so gestaltet sind, wie sie es eben sind. Das erhöht die Akzeptanz und damit die Wirksamkeit enorm. Bei der Ausgestaltung all dieser Maßnahmen, aber auch der dazugehörigen Unterweisungen, sollte immer eines bedacht werden: Ein Großteil der Belegschaft beschäftigt sich hauptberuflich nicht mit Cybersecurity. Dementsprechend verständlich müssen alle Maßnahmen erklärt werden. Außerdem ist darauf zu achten, dass sie im Arbeitsalltag auch umsetzbar sind. Kurz gesagt: Es gilt eine Balance zwischen Schutz und Usability zu finden.

Technik ermöglicht es, Cybersecurity-Niveau aufrecht zu erhalten

Glücklicherweise bietet der Markt mittlerweile etliche technische Möglichkeiten, die dabei unterstützen, ein gutes Cybersecurity-Niveau aufrecht zu erhalten. Das fängt bei der Firewall an, wird durch verschiedene Systeme zum Monitoring sowie zur Angriffserkennung und Angriffsverhinderung (IDS und IPS) unterstützt. Leider lässt sich keine allgemeingültige Aussage treffen, für welchen Fall welche Systeme und Vorkehrungen am geeignetsten sind. Das ist immer abhängig von den Gegebenheiten. Sicher ist aber, dass es für jeden Bedarf ein passendes Konzept gibt, das mit einem ökonomisch sinnvollen Aufwand den bestmöglichen Schutz bietet.

Einzig die Verfügbarkeit von entsprechend qualifizierten Mitarbeitenden könnte ein Problem darstellen. In diesem Fall unterstützen externe Dienstleister, wie Telent, die Managed Security Services anbieten und vom Patch-Management, über das kontinuierliche Monitoring der vorhandenen Netzwerke bis hin zu Handlungsempfehlungen die komplette Cybersecurity-Palette, etwa mit einem eigenen SOC (Security Operations Center), abdecken. Auf das die Passagiere – nicht nur aus den hier genanntem Beispielen – immer problemlos ihr Ziel erreichen. ■

Jakob Schmidt, Coordinator Awareness Koramis im Kompetenzzentrum für Cybersecurity der Telent GmbH.

telent GmbH:
www.telent.de