Bild: Andreas Eicher

Geradeaus ins Verderben? Wohin geht die Reise beim Thema Cybersicherheit und Big Data?

Unsere anfällige Welt im 4.0-Modus

Früher war bekanntlich immer alles besser. Wer in der Vergangenheit das Haus verließ, der schaltete das Licht aus, um Strom zu sparen. Oder ein, damit mögliche Einbrecher abgeschreckt werden. Auch das Auto wurde manuell im Handbetrieb mit Lenkrad gesteuert. Ganz zu schweigen von den Ordnern, die man in die eigenen Regale stellte, um wichtige Dokumente darin aufzubewahren.

Autor: **Andreas Eicher**

Heute ist vieles smart, sprich intelligent, weil digital und vernetzt. Egal, ob Industrie, die Energie- und Automobilwirtschaft, Banken, Versicherungen oder die private Dateiablage in der „eigenen Wolke“: Analog ist out. So redet uns das vielfach die Werbeindustrie ein. Das heißt: Wer nicht digital mithält, immer das neueste Gerät, die schnellste Datenleitung oder smarteste App zur Hand hat, ist raus. Welche Stilblüten das Ganze treibt, offenbart sich beispielsweise

beim Anruf des Mobilfunkanbieters. Spracherkennung soll den Kunden lenken, automatisiert versteht sich. Ob die Auswahlmöglichkeiten zwischen Vertragsänderung, Umzug oder Mobilfunk die richtigen sind, spielt keine Rolle und entpuppt sich im Praxisbetrieb oft als lästig. Denn was „Alexa" kann mit „Alexa, setz bitte Hundefutter auf die Einkaufsliste", ist in der Realität nicht immer so einfach.

Die Einfallstore für Hacker und Datendiebe

Jüngst zeigte sich bei der Fluglinie „British Airways", wohin all die Digitalisierung und Automatisierung führt. Ein Stromausfall in der IT sorgte für massive Flugausfälle. Die Folge: gestrandete Passagiere in London und weltweit an den Flughäfen. Der Kosten- und Imageschaden dürfte immens sein. Wer erinnert sich nicht an den kürzlich umhergeisternden Krypto-Trojaner „WannaCry", der unzählige Rechner weltweit infizierte, Krankenhäuser lahmlegte und die Autoproduktion im Nachbarland Frankreich störte. Die Ursachen für solche Ausfälle und Angriffe sind vielfach hausgemacht.

Einerseits werden viele Mitarbeiter noch immer nicht ausreichend geschult und sensibilisiert, wenn es um die Cybergefahren in der eigenen Organisation geht. Andererseits herrscht in vielen Produktionsbetrieben Old-School-Technologie in der Fertigung vor. Zu lange haben sich die Verantwortlichen darüber keine Gedanken gemacht. Dafür umso mehr die Hacker. Für die sind solche Schwachstellen die Einfallstore in Unternehmen. Regelmäßig zeigen Experten auf Messen und Kongressen, wie einfach es ist, von außen in Industrieanlagen einzudringen. Mit wenigen Handgriffen lassen sich so Windanlagen manipulieren, die Wassertemperaturen in Babybecken von Schwimmbädern nach Gusto erhöhen oder senken, smarte Autos kapern sowie Stromversorgungen unterbrechen.

Die, die es wissen oder managen sollten, wissen es nicht besser

Nun haben Unternehmen und ihre Führungsmannschaften eine gewisse Aufsichtspflicht in puncto funktionierender Prozesse und Sicherheitsstrukturen. Ihnen obliegt die Verantwortung, den ordnungsgemäßen (Produktions-)Ablauf sicherzustellen sowie die Wirksamkeit der eingesetzten Maßnahmen regelmäßig zu überprüfen und gegebenenfalls neu zu justieren. Doch das Gegenteil ist der Fall. Pleiten, Pannen und Zwangspausen sind keine Seltenheit in Unternehmen – sei es aufgrund ausfallender IT-Systeme, wegen eines Hackerangriffs oder weil der Zulieferer in die Knie geht. Unsere global vernetzte Welt im modernen 4.0-Modus ist anfällig. Und in diesem Zuge können auch nationale Behörden, wie das Bundesamt für die Sicherheit in der Informationstechnik (BSI), wenig ausrichten. Der Angriff auf die IT des Deutschen Bundestags offenbarte die Machtlosigkeit gegen professionelle Hackerangriffe. Auch das Gesetz zum Schutz kritischer Infrastrukturen ist nicht mehr als Fassade. Meldewesen gegen moderne Cyberkriege. Das wirkt nach Behörde, wenig durchdacht. So zeigt sich, dass die, dies es wissen oder managen sollten, es nicht besser wissen. Nun hat nach Bekanntwerden des WannaCry-Angriffs das BKA die Ermittlungen übernommen. Auch das wirkt eher nach Aktenzeichen XY… ungelöst" zu Zeiten Eduard Zimmermanns. Die Erfolgsquote der Ermittler dürfte gegen Null tendieren.

Hinter solchen Angriffen stehen meist gut organisierte Teams, von Staaten gelenkt oder privatwirtschaftlich aufgestellt. Längst haben Staaten und kriminelle Organisationen erkannt, dass Datenklau sowie Sabotage lohnende Geschäfte sind. Sei es, um andere Staaten in Misskredit zu ziehen oder staatliche Interessen im Cyberraum durchzusetzen oder sei es aufgrund rein wirtschaftlicher Interessen, dem Hacken von Daten und deren Verkauf.

Geodaten sind lukrativ – für Staaten und Unternehmen

In diesem Kontext bilden Geodaten-basierte Systeme ein besonderes Einfallstor. Einerseits für staatliche Stellen: Bewegungsprofile sowie Überwachung stehen ebenso im Fokus wie die analytische Verwertung großer Datenmengen – zur Gefahrenabwehr und -prävention. Nicht umsonst entstehen in immer mehr Städten durchgängige Überwachungseinrichtungen im öffentlichen Raum, um beispielsweise Passanten auf Schritt und Tritt zu überwachen. Wie weit das führen kann, zeigt ein Blick nach London oder auf das Berliner Südkreuz mit intelligenter Videoüberwachung. Das Online-Portal des Rundfunk Berlin-Brandenburg (rbb) schreibt im Rahmen einer Ausstellung „Watched!" zur Überwachung: „Der Mensch wird ständig beobachtet. Videokameras an öffentlichen Plätzen sowie in Gebäuden zeichnen all seine Bewegungen auf. Und er selbst füttert Big Data bereitwillig mit privaten Daten, etwa auf Facebook oder Instagram" [1]. Andererseits stehen Digitalunternehmen diesem Treiben in nichts nach. Sie sind ebenso an Geoinformationen und deren Auswertung im Bereich von Business und Location Intelligence interessiert.

Schließlich ist die Analyse und sinnstiftende Verknüpfung großer Datenmengen ein Riesengeschäft. Der gläserne Kunde ist längst Realität und die digitalen Geschäftsmodelle setzen verstärkt auf Geodaten. Klar ist, dass Geoinformationen eine wichtige Komponente bei Analysen spielen, beispielsweise für Versicherungen und das Gesundheitswesen. Sei es, um Naturrisiken und deren Schadensmaße vorauszusehen oder die Versorgung kranker Menschen im Alltag besser zu steuern. Viele weitere gute Beispiele ermöglichen einen sinnvollen Geoinformationseinsatz.

Wenn aber die reine Datensammlung unter dem Deckmantel der Terrorbekämpfung im Mittelpunkt steht sowie Informationen zu Marketing- und Verkaufszwecken „missbraucht" werden, dann läuft etwas falsch. Alexa, Google & Co lassen grüßen.

Quelle:

[1] www.rbb-online.de/stilbruch/archiv/20170223_2215/ausstellungen-ueberwachung-fotografie-watched.html