

Industrial Cyber Security Aktuell

Newsletter zur Sicherheit hoch automatisierter Produktionsanlagen • 05/2009

Langner
PRODUCTION BUSINESS

Furcht, Ungewissheit und Zweifel

Fear, Uncertainty and Doubt – das sind die Todsünden der vertrieblichen Argumentation für Sicherheitsprodukte, sagt man. Warum Furcht, Ungewissheit und Zweifel aber sehr viel mehr mit Industrial Cyber Security zu tun haben als nur mit hilflosem Verkäufergeschwätz, erfahren Sie in dieser Ausgabe des Newsletters. **Ralph Langner, Langner Communications GmbH**

Wie manchmal für IT-Sicherheitsprodukte geworben wird, da kann einem schon Angst und Bange werden – Horrorszenerarien werden an die Wand gemalt, in der Hoffnung, der armen Kundenseele mit dem Versprechen, mit Produkt X und Dienstleistung Y könne er künftig ruhig schlafen, einen Auftrag aus dem Ärmel zu leiern. Leider suchen zu viele Anbieter ihr Heil darin, die Bedrohungslage über alle Maßen zu dramatisieren. Unabhängig von diesem Getöse, an das man sich schon einigermaßen gewöhnt hat, gehören Furcht, Ungewissheit und Zweifel aber von Hause aus zum Security-Geschäft dazu. Das schauen wir uns einmal genauer an.

Ungewissheit

Ungewissheit ist mit Security so untrennbar verbunden wie der Begriff Risiko. Ungewissheit bedeutet hier: Wir wissen nicht, was kommt – wir bewegen uns im Bereich der Vorhersage. Und wie bereits der Satiriker Karl Kraus treffend formulierte, sind Prognosen schwierig, vor allem, wenn sie auf die Zukunft gerichtet sind. *Wo von Risiko die Rede ist, gibt es keine Gewissheit.* Wo Gewissheit herrscht, spricht man nicht von **Risiko**, sondern von **Schicksal**. Die Ungewissheit, wann ein Schadensfall eintritt und wie hoch der Schaden dann ausfällt, ist somit ein Konstituens des Sicherheitsbegriffs überhaupt.

Dieser einfache Zusammenhang ist leider selbst Fachleuten nicht unbedingt klar. So gab zum Beispiel Günter Ennen vom Bundesamt für Sicherheit in der Informationstechnik (BSI) in einer „vom ZVEI-Fachverband Automation ins Leben gerufenen Expertenrunde aus Safety- und Security-Spezialisten“ unlängst zu Protokoll: „Wenn nichts passiert, ist alles erreicht“ (etz 4/09). So denken ja auch viele Betreiber: Bisher ist nichts passiert, also sind wir sicher, frei nach Artikel 3 des **Kölsche Grundgesetz**: *Et hätt noch immer jot jejange*. Eigentlich hätte man erwartet, dass zumindest die anwesenden Safety-Spezialisten Ennen ins Wort fallen, da eine verrottete Anlage jenseits der Zertifizierbarkeit, die eigentlich sofort abgeschaltet gehört, ja nicht dadurch sicher wird, dass bisher nichts passiert ist.

Sicherheit gibt es nur dort, wo – nach sorgfältiger und sachgerechter *Prüfung* – nichts passieren *kann*. Ob etwas passieren würde, wenn man nichts täte, oder ob man einfach Glück hätte und

deshalb schadensfrei ausginge – das ist und bleibt eben *ungewiss*, ebenso wie die Frage, ob etwaige Sicherheitsmaßnahmen aus der Rückschau betrachtet überhaupt erforderlich waren – erinnert sei an eine vorangegangene Ausgabe dieses Newsletters mit dem Titel „Kassandra, Rosi, und die Finanzkrise“. Das ist unbefriedigend, da ein Entscheider bei den so verursachten Kosten für Sicherheitsmaßnahmen nicht wissen kann, ob sie vermeidbar gewesen wären – aber es ist leider nicht zu ändern, wenn man ein gewisses Sicherheitsniveau erreichen und halten will. Sicherheit und Ungewissheit lassen sich nicht auseinander dividieren. Schutzmaßnahmen sind gerade deshalb erforderlich, weil ein schadensfreier Betrieb ungewiss ist. Wo das anders ist, werden sie nicht gebraucht – entweder weil sowieso nichts passieren kann, oder weil ein Schaden gewiss wäre und die Anlage somit von vornherein gar nicht in Betrieb genommen wird.

Zweifel

Der Betreiber zweifelt beim Thema Cyber-Sicherheit an mehreren Dingen. Erstens bezweifelt er, dass bei ihm überhaupt ein Sicherheitsvorfall eintritt – das ist ja schließlich *ungewiss* –, und zweitens, dass sich Aufwendungen für Sicherheitsmaßnahmen irgendwie betriebswirtschaftlich „rechnen“ könnten. Er bezweifelt möglicherweise sogar ganz grundsätzlich, dass man sich mit so einem Orchideenthema wie Cyber-Sicherheit überhaupt beschäftigen müsse, denn schließlich hat man sich in den letzten zehn, zwanzig Jahren da ja auch nicht drum gekümmert, und passiert ist – anscheinend – nichts. (Kölsche Grundgesetz, Artikel 6: *Kenne mer nit, bruche mer nit, fott domet.*)

Die Anbieterseite tut das ihrige hinzu, um solche verständlichen Zweifel zu befördern. Wer penetrant eine Gefahr durch Hacker beschwört, die nicht belegbar ist, sät nun mal Zweifel an seiner Seriosität. Haben Sie in diesem Zusammenhang schon mal den Namen Vitek Boden gehört? Das ist der Kronzeuge der Hacker-Beschwörer. Boden hatte nämlich vor neun Jahren mutwillig durch Cyber-Manipulation einer Kläranlage Abwasser in die Umwelt geleitet. Unappetitlich das Ganze, aber der wirtschaftliche Schaden war

letztendlich marginal. Der Fall Vitek Boden ist hinsichtlich des Schadensausmaßes so unbedeutend, dass man vermutlich nie etwas davon gehört hätte, wenn es noch andere dokumentierte Fälle von Cyber-Sabotage geben würde. Die gibt es aber nicht. Insider kennen zwar noch weitere Fälle, aber hier reden wir nicht von Hunderten oder gar Tausenden von Vorfällen, sondern eher um eine zweistellige Zahl im mittleren Bereich – weltweit, über den Zeitraum der letzten zehn Jahre (vorher gab es ohnehin keine Vernetzung im nennenswerten Ausmaß). Die durch diese Vorfälle hervorgerufenen Schäden waren durchweg minimal, also allenfalls im fünfstelligen Euro-Bereich. Bei einer Grundgesamtheit von mehreren Hunderttausend potenziell betroffenen Einrichtungen kann man sich als mittelständischer Betreiber dann ausrechnen, dass das Risiko, Opfer so eines Cyber-Angriffs zu werden, nicht groß genug ist, um gleich nächste Woche mal einen Security-Consultant mit saftigem Honorar- und Spesensatz zu beauftragen. Die Zweifel des Betreibers sind in diesem Punkt also berechtigt.

Da gibt es dann allerdings eine Situation, die schlagartig alle Zweifel ausräumt: Wenn nämlich im eigenen Werk ein Sicherheitsvorfall passiert. Dann kommt die Erkenntnis, dass Cyber-Sicherheit nicht auf die leichte Schulter genommen werden kann, dass doch nicht alles Quatsch war. In der Regel handelt es sich dabei dann natürlich nicht um Hacker-Angriffe, sondern um einen Vorfall aufgrund einer nicht-intentionalen Bedrohung, die treue Leser dieses Newsletters zur Genüge kennen und die bei wachsender Vernetzung ohne vernünftige Security-Prozeduren nur eine Frage der Zeit sind. Mancher übersieht, dass Sachverhalte, deren Relevanz man zunächst mit Fug und Recht bezweifeln mag, allein durch diesen Umstand nicht unreal werden. Vom Bezweifeln zum Verdrängen ist der Weg zuweilen kurz.

Furcht

Auch heute noch versuchen Anbieter von Sicherheitsprodukten und –dienstleistungen Angst zu schüren; so manche werbliche Argumentation läuft ungefähr darauf hinaus, dass Schutz vor bösen Geistern verkauft werden soll. erinnert sei hier an eine frühere Ausgabe dieses Newsletters mit dem Titel **Voodoo Security**. Nimmt man das Angebot an, als Schutzgeldzahlung sozusagen, erkaufte man sich damit wohl Angstfreiheit. Nun ist Angst aber nicht dasselbe wie Furcht. Die Klinische Psychologie unterscheidet hier feinsinnig zwischen der Angst, die sich rational nicht begründen lässt und somit pathologische Züge trägt (z.B. Angst vor Spinnen, Angst in engen Räumen, Höhenangst, Angst vor Cyberterroristen) und der gesunden Furcht, die eine rationale Grundlage hat und objektiv berechtigt ist (z.B. Furcht, sich anzustecken, wenn der Kollege am Schreibtisch gegenüber ständig niest, Furcht vor Jobverlust in der Wirtschaftskrise usw.). Während Angst immer ein schlechter Ratgeber ist, ist das bei Furcht meist andersherum – sie leitet an zur Vermeidung potenziell gefährlicher Situationen.

Egal, wie sehr ihnen das manche Anbieter und Journalisten auch einreden wollen: Die Betreiber haben durchgängig keine Angst beim Thema Cyber-Sicherheit. Sie haben Furcht. Und diese Furcht der Betreiber ist so banal wie berechtigt. Der Betreiber fürchtet nicht den

(möglicherweise desaströsen) Schaden durch Sicherheitsvorfälle, weil er die ja sowieso für völlig unwahrscheinlich hält. *Er fürchtet die Kosten, die mit allfälligen Sicherheitsmaßnahmen verbunden wären.* Es ist ja klar, dass das alles nicht zum Nulltarif kommt. Da er im tiefsten Innern ahnt, welche Leichen da aus dem Keller geräumt werden müssen, schwant ihm: Das wird teuer. Man liest das ja auch in der Presse. So zitiert beispielsweise die *Computerwoche* vom 8.2.2008 die Sicherheitsberaterin Susanne Ginschel vom Münchner Security-Anbieter *Defense AG* mit dem denkwürdigen Statement: „Sicherheit kostet unwahrscheinlich viel Geld“. Das muss doch beim Betreiber Furcht und Schrecken auslösen, oder etwa nicht? Nun führt diese Reaktion allerdings nicht wie anbieterseitig gewünscht zu Panik- und Hamsterkäufen von Firewalls, Intrusion-Prevention-Systemen und Notstromaggregaten, sondern, wie Psychologen das nennen, zu **Reaktanz**. Es kommt zu einer Art Trotzreaktion mit Vogel-Strauß-Effekt, ungefähr nach dem Motto: Jetzt kümmer dich erst recht nicht darum, basta. Man möchte von dem Thema nichts mehr hören, und zwar gerade *weil* man irgendwie weiß, dass da was dran ist, und sucht sich deshalb allfällige Gründe dafür, weshalb man sich „momentan“ damit nicht befassen möchte/kann/darf.

Wengleiche das Phantasieren von „unwahrscheinlich viel Geld“, das man als Anbieter sicher gern verdienen möchte, natürlich Unsinn ist, müsste mancher Betreiber, der sich bisher keinen Deut um Cyber-Sicherheit im Produktionsumfeld gekümmert hat, in der Tat erstmal eine ordentliche Stange Geld in die Hand nehmen, um den Karren aus dem Dreck zu bekommen – Geld, das natürlich nicht im Budget vorgesehen war. Warum sollte man das tun? Weil zu befürchten ist, dass bei weiterem Zuwarten alles nur teurer werden kann.

Über den Autor

Ralph Langner ist Gründer und Geschäftsführer von Langner Communications. Er verfügt über mehr als zwanzig Jahre Erfahrung mit Automatisierungstechnischen und IT-Systemen und ist ein international bekannter Security-Experte für Prozessnetze.

Industrial Cyber Security Aktuell · Impressum

Langner Communications GmbH, Foßredder 12, D-22359 Hamburg
Tel.: +49-40-609011-0, Fax: +49-40-609011-11, info@langner.com
HRB 108928 AG Hamburg, USt.-ID DE118673252, www.langner.com
V.i.S.d.P.: Ralph Langner (Geschäftsführer)