IT-Sicherheit messen und bewerten

Risiken in produktionsnahen IT-Systemen transparent machen

Der Einzug der Informationstechnologie in die Produktion zieht Anforderungen an IT-Sicherheit nach sich. Nicht die IT-Abteilung, sondern die Betriebsleitung ist mit den Prozessrisiken vertraut und trägt die Verantwortung dafür, die Sicherheit der produktionsnahen IT-Systeme nachzuweisen. Die zentrale Frage ist: „Wie sicher SOLL das Produktions-IT-System sein und wie sicher IST es tatsächlich?"

Erwin Kruschitz, Vorstand von Anapur

Eine Produktion ohne IT-Systeme ist heute nicht mehr vorstellbar. Mit der zunehmenden Vernetzung und Komplexität der IT-Landschaften sowie Schadensereignissen wie dem Enron-Skandal und 9/11, sind auch die gesetzlichen Anforderungen strenger geworden. SOX, Basel II und KontraG etc. verlangen, Informationen als Unternehmenswerte gegen Manipulation oder Verlust, zu schützen.

Betriebe der Prozessindustrie beheimaten zumeist eine Vielzahl kritischer Prozesse, die durch verschiedene IT-Systeme wie Automatisierungs-, Labor-, Planungs- und Qualitätssicherungssysteme etc. gestützt werden. Nicht unbedingt ein Schadensszenario wie die gezielte Manipulation einer Pharma-Rezeptur, sondern insbesondere der kurzzeitige Ausfall eines IT-Systems, kann schwerwiegende rechtliche und wirtschaftliche Folgen sowie Schäden für Mensch und Umwelt, nach sich ziehen.

Kann die Betriebsleitung nicht nachweisen, dass sie ihrer Verantwortung für IT-Sicherheit nachgekommen ist, droht bei einem Versicherungsaudit möglicherweise eine negative Bewertung. Kommt es zum Schadensfall, könnte sogar der Vorwurf der Fahrlässigkeit geltend gemacht werden.

„Gefühlte" vs. tatsächliche Sicherheit

Bei IT-Security-Maßnahmen steht in der Praxis nach wie vor die „klassische" Office-IT im Vordergrund. Im Produktionsumfeld ist aktuell eine steigende Sensibilisierung für IT-Sicherheit zu verzeichnen. Die aus dem Büroumfeld bekannten Risiko-Schemata können jedoch nicht auf die produktionsnahen IT-Systeme übertragen werden, ohne die spezifischen Anforderungen zu berücksichtigen. Das Ergebnis wäre eine vermeintliche oder „gefühlte" Sicherheit, die an den tatsächlichen Risiken jedoch vorbei geht.

Verfügbarkeit hat Priorität

Spricht man über „Sicherheit", ist es wichtig sich vor Augen zu führen, welche Schutzziele man verfolgt – für IT-Systeme im Wesentlichen: Vertraulichkeit, Integrität und Verfügbarkeit. Im Office-Bereich steht die Vertraulichkeit, der Schutz vor unberechtigtem Zugang zu Information, an erster Stelle. Während ein fünfminütiger Systemausfall im Büro meist tolerierbar ist, kann er in der Produktion schwerwiegende Konsequenzen haben. Im Produktionsbereich hat deshalb Verfügbarkeit, die Aufrechterhaltung der Systemfunktion, Priorität.

Abb. 2: In produktionsnahen IT-Systemen steht der Schutz der Verfügbarkeit (Availability) an erster Stelle. Quelle: ISA 99

Abb. 1: Nicht Absturz und Erfrieren, sondern Herzversagen ist die häufigste Todesursache beim Bergsteigen. Auch für produktionsnahe IT-Systeme gilt: Die offensichtlichen Risiken sind nicht unbedingt die gefährlichsten. Quelle: © www.photocase.com

Jede zusätzliche Komponente reduziert die Verfügbarkeit des Gesamtsystems und macht es anfälliger. Das gilt für unnötige Office-Anwendungen in der Produktion – E-Mail Clients gehören nicht auf Prozessleitsysteme – ebenso wie für technologische Maßnahmen der „klassischen" IT-Security. Eine Firewall beispielsweise ist mit zunehmender Vernetzung auch in der Produktion sinnvoll, setzt aber gleichzeitig die Verfügbarkeit des Gesamtsystems herab. Eine sorgfältige Abwägung ist daher erforderlich.

„Wir sind sicher! – darum kümmert sich unsere IT-Abteilung". Oft wird die Verantwortung für die Sicherheit produktionsnaher IT-Systeme an die IT- oder Technik-Abteilung abgegeben. Diese ist jedoch nicht zwangsläufig mit den besonderen Anforderungen der Produktion vertraut. Zudem trägt die rechtlichen Konsequenzen letztendlich die Betriebsleitung oder Geschäftsführung, nicht die IT-Abteilung.

Wie sicher ist mein IT-System?

Seiner Verantwortung gerecht zu werden bedeutet, die Sicherheit des Systems beurteilen zu können. Wie aber misst man Sicherheit? Üblicherweise werden durch Assessments Risiken transparent gemacht und Sicherheitsmaßnahmen bewertet. Das Assessment beginnt mit einer Strukturanalyse, in der schützenswerte Prozesse und Objekte definiert und deren jeweiliger Schutzbedarf hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit festgestellt werden. Anschließend werden Bedrohungen, deren Eintrittswahrscheinlichkeit sowie mögliche Folgen anhand von typischen Schadenszenarien analysiert und die Wirksamkeit bestehender Sicherheitsmaßnahmen bewertet. Den Stand der Technik spiegeln dabei neben der nationalen VDI-Richtlinie 2182 „Informationssicherheit in der Automatisierung" des Namur NA 115, vor allem die international anerkannten Regelwerke ISO 27.000 und ISA 99 wider.

Wissen, worauf es ankommt

Um zwischen vermeintlichen und tatsächlichen Risiken unterscheiden zu können und auch weniger offensichtliche Gefahren zu erkennen, sind Expertise in den Bereichen Produktion, IT und Automatisierung unverzichtbar. Denn nur wer die Prozesse versteht, kann die Kritikalität von einzelnen Komponenten bewerten.

Um der Gefahr von Betriebsblindheit oder Voreingenommenheit auszuweichen werden Assessoren beauftragt, die sowohl vom Lieferanten als auch von internen Abteilungen unabhängig sind. Je unabhängiger der Assessor, desto aussagekräftiger das Assessment.

Faktor Mensch

Auch wenn Virenschutz und Firewalls in der Diskussion dominieren, gilt: Vor allem dem Faktor Mensch muss Rechnung getragen werden, denn er stellt nachweislich das größte Risiko dar. Technische Maßnahmen allein nützen nichts, wenn IT-Sicherheit nicht auch gelebt wird. Deshalb müssen insbesondere organisatorische Parameter betrachtet werden: Sind die Mitarbeiter für IT-Sicherheit sensibilisiert? Werden sie entsprechend geschult? Gibt es Arbeitsanweisungen? Werden Verantwortliche klar benannt?

Fazit

Die Produktions-IT steht vor der Herausforderung, die Sicherheitsfrage, vor dem Hintergrund komplexerer Systeme und strengerer gesetzlicher Anforderungen, möglichst effizient zu beantworten. Dabei zwischen vermeintlichen und tatsächlichen Risiken zu unterscheiden, ist nicht einfach. Ein IT-Security-Assessment durch produktionsnahe Experten macht Stärken und Schwächen transparent und bildet so die Entscheidungsgrundlage dafür, Maßnahmen gezielt einzusetzen. Der dokumentierte Nachweis über ein neutrales Assessment gibt Behörden, Versicherungen, Kunden oder im Schadensfall dem Staatsanwalt, eine klare Antwort auf die Frage nach der Sicherheit des Produktions-IT-Systems.

■ Kontakt:
Erwin Kruschitz
Anapur AG, Ludwigshafen
Tel.: 0621/62900-432
Fax: 0621/62900-431
e.kruschitz@anapur.de