SICHERE PRODUKTIONSUMGEBUNG

IT-Sicherheit in der Investitionsgüterindustrie

Situation im Maschinenbau

In der Investitionsgüterindustrie basieren die Arbeits- und Geschäftsprozesse immer stärker auf IT-Lösungen. Ohne die Unterstützung dieser Technik sind international agierende Unternehmen kaum noch existenzfähig. Die Vernetzung zwischen den Unternehmen und der Austausch von Informationen nehmen zu. Diese Art der Infrastruktur schließt feste, schnurlose und mobile Einrichtungen ein. Art, Umfang und Sensibilität der ausgetauschten Informationen haben wesentlich zugenommen. Die dadurch wachsende Verwundbarkeit ungeschützter IT-Einrichtungen und die Gefahr massiver wirtschaftlicher Schäden in Folge von IT-Risiken erhöhen den Handlungsdruck, eine Sicherheitsstrategie im Unternehmen zu entwickeln und umzusetzen. Zusätzlicher Handlungsdruck kommt verstärkt von Außen. Datensicherheit und IT-Sicherheit im Unternehmen werden zunehmend ein Entscheidungsfaktor für Auftraggeber (z.B. die Automobilindustrie), Banken, Wirtschaftsprüfer (Basel II-Kriterien, KonTraG, etc.) und für verbundene Unternehmen. Die IT-Sicherheit wird daher bei den erfolgreichen Maschinenbau-Unternehmen nicht als isolierter Aspekt, sondern als Teil des ganzheitlichen Riskmanagements im Unternehmen angesehen. Unternehmen, die durch Nachlässigkeit im Bereich IT- Sicherheit auffallen, gelten auch in unserer Branche inzwischen als „Risikofaktor" in der Zusammenarbeit bzw. bei der Auftragsvergabe.

IT-Sicherheitskosten

Eine weit verbreitete Ansicht ist, dass IT-Sicherheit zwangsläufig mit hohen Investitionen in Sicherheitstechniken und Beschäftigung von hoch qualifiziertem Personal verbunden ist. IT-Sicherheit muss jedoch als integraler Bestandteil der gesamten IT im Unternehmen gesehen werden. In Abhängigkeit des Schutzbedarfs muss für eine funktionierende IT kontinuierlich ein angemessenes Budget zur Verfügung stehen, das auch die Investitionen für IT-Sicherheit beinhaltet. Investitionen z.B. in Firewalls und Antiviren-Software sind heute selbstverständlich. IT-Services ohne Sicherheitsmaßnahmen sind wenig sinnvoll. Ein systembedingter Produktionsausfall kann z.B. schnell die jährlichen Kosten für die IT übersteigen, deren integrale Sicherheitsmaßnahmen den Ausfall hätten verhindern können (zzgl. Konventionalstrafen, Lieferverzögerung, Image- und Vertrauensverlust).

Die wichtigsten Erfolgsfaktoren für IT-Sicherheit sind jedoch gesunder Menschenverstand, durchdachte organisatorische Regelungen und zuverlässige, gut informierte Mitarbeiter, die selbständig Sicherheitserfordernisse diszipliniert und routiniert beachten. Technische Maßnahmen und Geräte sind dann die Umsetzung der Sicherheitsstrategie im Unternehmen, wo organisatorische und rechtliche Maßnahmen nicht mehr greifen.

Da der Hauptgrund für Sicherheitslücken nach Erfahrung vieler Unternehmen gerade das fehlende Sicherheitsbewusstsein der eigenen Mitarbeiter ist, muss im eigenen Unternehmen mit der Aufklärungsarbeit anfangen werden. Die Geschäftsführung ist aufgefordert, sich einen Überblick über den Schutzbedarf und die Bedrohung für die jeweiligen Bereiche verschaffen und die Mitarbeiter entsprechend zu sensibilisieren. So sollten z.B. vertrauenswürdige Informationen (wie Konstruktionszeichnungen oder Angebote und Verträge) nicht unverschlüsselt per E-Mail versendet werden. Bedeutend ist, dass das Management mit gutem Beispiel voran geht.

IT-Sicherheit ist Chefsache

Nicht nur Know-how-Schutz, Datenschutz und die Sicherheit von Kundenaufträgen erfordern erhöhte Schutzmechanismen. Die erfolgreiche Zusammenarbeit zwischen Geschäftsführung und IT-Verantwortlichen trägt auch den geänderten Gesetzen Rechnung, die bei Versäumnissen eine persönliche Haftung der Geschäftsführung vorsehen, wenn es zu einer Gefahr für das Unternehmen durch mangelnde IT-Sicherheit kommt. IT-Sicherheit ist somit Chefsache. Die Geschäftsführung muss den Sicherheitsprozess im Unternehmen initiieren, vorantreiben und kontrollieren.

IT-Sicherheit erreichen und weiterentwickeln

Folglich ist IT-Sicherheit keine rein technisch zu betrachtende Unternehmensangelegenheit. Vielmehr sind juristische, organisatorische und personelle Aspekte zu berücksichtigen. Demnach kann eine ausschließliche Betrachtung der technischen Sicherheit keine Aussage über die Sicherheit im Unternehmen machen. Aus diesem Grund darf Unternehmenssicherheit nicht alleinige Aufgabe der IT-Abteilung oder gar eines einzelnen Netzwerkadministrators sein.

Die Erstellung und technische Umsetzung eines Sicherheitskonzeptes, die regelmäßige Information über Sicherheitsmängel und entsprechende Lösungsvorschläge ist Aufgabe des IT-Verantwortlichen, ebenso wie die Beantragung eines angemessenen Budgets für die Erreichung eines notwendigen Sicherheitsstandards. Die Verantwortung für die IT-Sicherheitsstrategie und deren Umsetzung aber liegt bei der Geschäftsführung. Für IT-Sicherheit zu sorgen bedeutet auch, eine ganzheitliche Gefährdungs- und Risikoanalyse zu erarbeiten. Das Sicherheitskonzept muss organisatorische, technische und personelle Maßnahmen umfassen! Ergo muss das ganze Unternehmen mit seinen Geschäftsprozessen und die Einbettung in eine Wertschöpfungskette berücksichtigt werden.

Hier wird deutlich, dass IT-Sicherheit ein Bestandteil des Riskmanagements im Unternehmen ist und nicht losgelöst gesehen werden darf. Das gilt auch für die Kosten. Bei der Umsetzung einer zwingend erforderlichen Sicherheitsstrategie im Unternehmen kann der neue VDMA-Leitfaden eine wertvolle Einstiegshilfe sein. Sicherheit ist, unabhängig von der Unternehmensgröße, ein immer wichtigeres Thema im Maschinenbau, vor allem wenn es darum geht, Forschungs- und Entwicklungsdaten sowie Kundenaufträge effektiv zu schützen. Der Leitfaden hilft, Gefahrenquellen zu identifizieren, Schutzbedarf festzustellen, gibt Handlungsempfehlungen und ermöglicht einen Vergleich mit dem Branchenstatus. Er nimmt im wesentlichen Bezug auf das Grundschutzhandbuch (GSHB) des Bundesamt für Sicherheit in der Informationstechnik (BSI) und bietet eine erste Orientierungshilfe. Das Grundschutzhandbuch wurde als Grundlage ausgewählt, da es sich auch in unserer Branche als geeignetes Instrument erwiesen hat, in das Thema IT-Sicherheit einzusteigen und eine Sicherheitsstrategie im Unternehmen einzuführen. Alternativ kann auch der britische Standard BS 7799 oder andere Kriterienwerke herangezogen werden.

Wichtig ist, dass eine Sicherheitsstrategie / -konzept im Unternehmen eingeführt und gelebt wird!

Jens Geißmann
VDMA
LV Baden-Württemberg

Easy Info • 266