

Sicherheit ohne Fundament?

Kritische Infrastrukturen, Geschäftsprozesse und die Sicherheit

(BS) Die Bedeutung der elektronischen Datenverarbeitung ist in der modernen Dienstleistungsgesellschaft nicht mehr zu vernachlässigen. Kritische Infrastrukturen wie Versorgungsnetze (Strom, Wasser, Energie, Verkehr, Kommunikations- und Datennetze) und öffentliche Verwaltung (Melde- und Fahndungssysteme, digitaler Polizeifunk etc.) werden mit Geräten und Verfahren der Informationstechnik gesteuert und betrieben. Alle Geschäftsprozesse in Industrie und Verwaltung werden mit moderner Informationstechnologie unterstützt. Ein Ausfall dieser Informationssysteme wäre kritisch, unentdeckte oder gegebenenfalls sogar gezielte Veränderungen an diesen Informationssystemen hätten katastrophale und ggf. viel zu spät entdeckte Folgen.

Die Bedeutung der Sicherheit dieser Informationssysteme steht daher außer Frage. Doch umfassende Sicherheit gibt es nicht als fertiges Produkt zu kaufen. Stattdessen müssen Sicherheitskonzepte entwickelt und mit entsprechenden Lösungen für die Informationstechnik umgesetzt werden. Das kostet Geld, denn Sicherheit war noch nie billig. Deswegen verwundert es, wenn in vielen EDV-Abteilungen teure Sicherheitskonzepte entwickelt und umgesetzt werden, ohne dass eine Grundlage im Sinne eines modernen Konfigurationsmanagements gegeben ist. Man kann den Eindruck gewinnen, dass bei Sicherheitskonzepten in das hoch sichere Schloss der Eingangstür investiert wird, ohne eine Bauzeichnung oder einen Bauplan zu haben, der einem zeigt, wo weitere "Schlupflöcher" sind.

Konfigurationsmanagement

Ein modernes Konfigurationsmanagement für Informationssysteme ist für sich genommen natürlich keine Sicherheitslösung. Eines ist jedoch klar: wenn der Betreiber und Verantwortliche für diese Informationssysteme nicht jederzeit einen vollständigen und aktuellen Überblick über alle Geräte und deren Konfigurationen besitzt, dann kann kaum von einer sicheren Umgebung gesprochen werden. Das Dilemma für die EDV-Verantwortlichen ist dabei, dass sie wenig Einfluss auf die Art und die Häu-

figkeit von Veränderungen im EDV-Umfeld haben. Am besten wäre es für den EDV-Betreiber, wenn die Informationssysteme möglichst lange in dem eingerichteten und zum Sicherheitskonzept passenden Zustand verbleiben. Aber man denke zum Beispiel allein an die Flut der Sicherheitsmitteilungen der Betriebssystemhersteller, denen der EDV-Verantwortliche nachkommen muss, oder die Veränderungen durch die oft jährlichen Aktualisierungen der Anwendungen. Diesen Veränderungen kann und darf sich der EDV-Betreiber nicht entziehen. Aber jede Aktualisierung einer Anwendung kann ein Sicherheitskonzept unterlaufen. In dieser Ausgangslage wird ein modernes Konfigurationsmanagement für die Informationstechnik unverzichtbar. Wenn schon die Häufigkeit der Veränderungen nicht reduziert werden kann, muss wenigstens der jeweilige Zustand der Informationssysteme über die Zeit dokumentiert werden. Zusätzlich müssen die entstandenen Veränderungen aufgezeigt werden und ein Abgleich der Konfigurationen und Versionen mit den Sicherheitsempfehlungen der jeweiligen Hersteller durchgeführt werden.

Intelligente Automatisierung

Die Lösung für die EDV-Verantwortlichen bietet ein modernes Konfigurationsmanagement für die Informationssysteme mit hohem Automa-

tisierungsgrad. Dieses Konfigurationsmanagement stellt das Fundament für einen effizienten und sicheren EDV-Betrieb dar. Und dabei sind Effizienz und Sicherheit kein Widerspruch, sondern es sind die Ergebnisse eines sinnvollen Lösungsansatzes. Das Konfigurationsmanagement verwaltet alle Geräte und Anwendungen der EDV-Umgebung, und dokumentiert dies regelmäßig, zum Beispiel einmal pro Nacht. Damit keine Geräte unerkannt bleiben, bietet das Konfigurationsmanagement eine netzwerkgestützte Erkennungsfunktion, mit der neue Geräte im Netzwerk erkannt und gemeldet werden. Für alle Geräte werden die erfassten Informationen mit Zeitstempel und Prüfsumme versehen in einer Datenbank gespeichert, sodass eine automatische Veränderungsüberwachung durchgeführt werden kann, die dem EDV-Betreiber Veränderungen an den Geräten mitteilt. Zusätzlich sind im Konfigurationsmanagement die als sicherheitsrelevant definierten Versionsstände und Fehlerbereinigungen der Betriebssysteme und Anwendungen hinterlegt. Diese Vorgaben werden ebenfalls automatisch mit den Konfigurationsdaten der Geräte und Systeme abgeglichen und lösen bei Abweichungen Alarme aus.

Die drei Kernfunktionen eines modernen Konfigurationsmanagements von Informationssystemen müssen über Betriebssystemgrenzen hinweg

für die gesamte EDV-Umgebung bereitgestellt und umgesetzt werden. Und diese Funktionen müssen anpassbar sein, damit nicht Veränderungen an als unkritisch eingestuften Informationen eine unnötige Alarmierung auslösen.

Die Anforderungen an ein modernes Konfigurationsmanagement von Informationssystemen sind daher hoch:

- vollständige und aktuelle Geräte-, System- und Anwendungsinformationen,
- automatisierte und anpassbare Veränderungsüberwachung,
- automatisierter Soll-/Ist-Abgleich für Sicherheitshinweise und Sicherheitsaktualisierungen,
- Anpassbarkeit der Überwachungs- und Abgleichregeln,
- betriebssystemübergreifender, netzwerkweiter Ansatz.

eRunbook Security Console

In Kooperation mit der Secunet AG wurde daher die eRunbook Security Console entwickelt, welche die Anforderungen an ein modernes, effizientes und sicheres Konfigurationsmanagement von Informationssystemen erfüllt und für den Einsatz in Kritischen Infrastrukturen bereitsteht.

Weitere Informationen: secunet Security Networks AG, Michael Böffel, Tel.: 0201/5454-1050, E-Mail: Michael.Boeffel@secunet.com, novaratio AG, Georg Scherzinger, Tel.: 02623/ 9242-104, E-Mail: GS@novaratio.de