BSI-Vorgaben mit heutigen IT-Anforderungen in Einklang bringen

Compliance: Mehr Chancen als Widersprüche?

1993 auf den Weg gebracht, hat sich aus dem zwischenzeitig mehr als 4500 Seiten umfassenden IT-Grundschutz-Katalog dank Überarbeitung wieder eine überschaubarere Vorgabensammlung ergeben. Mit welch anspruchsvollen Aspekten daraus Kommunen und Behörden nach wie vor zu kämpfen haben, darauf geht Sicherheitsexperte Dennis Buroh im Interview ein.

Das BSI stellt hohe Ansprüche an öffentliche Einrichtungen mit der ISO 27001, basierend auf dem IT-Grundschutz. Was sind die wesentlichen Eckpunkte?

Buroh: Der IT-Grundschutzkatalog in Verbindung mit der ISO 2700X-Reihe sowie dessen Empfehlungen von Standard-Sicherheitsmaßnahmen stellt einen De-Facto-Standard für IT-Sicherheit dar. Seit 2006 werden daher ISO 27001-Zertifizierungen auf der Basis des IT-Grundschutzes durchgeführt. Im Basisschutzkonzept des BSI sind vier Hauptrisikofaktoren aufgeführt, die im besonderen Fokus stehen sollten, um den IT-Grundschutz einhalten zu können. Im Einzelnen sind das: der Mensch mit den Merkmalen „mangelndes Sicherheitsbewusstsein", „menschliches Versagen", „kriminelles Verhalten" und „Unachtsamkeit", die Organisation, z. B. im Hinblick auf das Outsourcing der internen IT, die Natur und Umwelt und die IT-Systeme, insbesondere was deren Abhängigkeiten und Komplexität angeht.

Nicht zu unterschätzen sind dabei der Faktor Mensch und

die vielen Angriffspunkte, die dieser bietet, selbst als privilegierter Nutzer des IT-Systems. Gerade bei einer ersten Annäherung an die Thematik der IT-Sicherheit sollten sämtliche aufgeführten Faktoren als Ausgangspunkte auf dem Weg zu einer sicheren IT-Struktur verstanden werden.

Was sind privilegierte Nutzer? Ist deren Überwachung nicht in sich ein Widerspruch?

Buroh: Ein privilegierter Nutzer ist ein Anwender, der volle Administrationsrechte auf einem System besitzt und daher all seine Aktivitäten verschleiern kann. Eine Verschleierung liegt vor, sobald der Anwender seine Spuren auf dem System löschen kann und in der Folge kein Nachweis mehr über dessen Tätigkeiten oder Handlungen existiert.

Allerdings kann ein Anwender auch ohne Administrationsrechte privilegiert sein. Dieser indirekt privilegierte Nutzer entsteht durch Lücken der Protokollierung von Aktionen in einer Software. In einer Finanzbehörde würde beispielsweise das Buchungssystem nicht mitloggen, welche Kontodaten angesehen wurden oder welche Grundbesitzer einen Ausstand bei den Steuern hatten. Unter dem Aspekt der Nachvollziehbarkeit der Datenveränderung und Datenverbreitung des Bundesdatenschutzgesetztes ist daher eine Überwachung und Protokollierung dieser privilegierten Nutzer – beziehungsweise Anwender – dringend geboten, möchte man datenschutzkonform handeln.

IT-Governance hat als oberstes Ziel, IT-Prozesse konsequent an der Gesamtstrategie auszurichten. Könnte es hier nicht Konfliktpotenzial im Zusammenhang mit den aktuellen Vorgaben des Bundesdatenschutzgesetzes (BDSG) geben?

Buroh: Im Gegenteil, aufgrund der neuen Europäischen Datenschutzgrundverordnung (DS-GVO) ist nun der Zeitpunkt zum Handeln gekommen. Diese neue Verordnung sieht eine Neuregelung des BDSG und von seiner Prozesse vor. Ab Mai 2018 ist die Kommune als Arbeitgeber in der Pflicht, nachzuweisen, dass die Mitarbeiter datenschutzkonform sämtliche Prozesse im Unternehmen eingehalten haben. Dies stellt eine erhebliche Anforderung und eine auf den ersten Blick kaum zu bewältigende Aufgabe dar. Allerdings ermöglicht eine korrekt konfigurierte Lösung eine unglaubliche Transparenz und gleichzeitige Kontrolle über Compliance-Anforderungen. Wichtig ist es daher zu wissen, welches Lösungssystem zu den eigenen Prozessen passt.

Rechtliche Anforderungen ändern sich ständig. Wie lassen sich da überhaupt Wirtschaftlichkeit und zeitgemäße Datensicherung in Einklang bringen?

Buroh: Ändern sich wirklich regelmäßig die Anforderungen? Die Grundanforderung und damit das Erreichen der IT-Schutzziele sind seit ewigen Tagen gleich geblieben: Vertraulichkeit, Verfügbarkeit und Integrität. Allerdings ändern sich die Technologien sowie unsere Arbeitsweise im Büroalltag regelmäßig. An diese Gegebenheit passen sich die Gesetzestexte stets an. Bei der Auswahl der Sicherheitslösung sollte man daher auf der sicheren Seite sein und nicht in ein hochspezialisiertes Nischensystem investieren, das nur einen kleinen Prozessteil der eigenen IT-Landschaft abdecken kann oder eine komplette Umstellung meiner Arbeitsweise im Büro voraussetzt.

Fast immer lässt sich Datenschutzkonformität schon durch kleinste Maßnahmen ermöglichen, die keine Auswirkungen für den Endanwender und dessen Arbeitsweisen nach sich ziehen. Hierdurch ist auch eine Wirtschaftlichkeit gewährleistet und Mitarbeiter benötigen keine erneute Umgewöhnung an neue Prozesse oder Systeme.

Dennis Buroh ist Security Consultant und internationaler Projektmanager bei der Consist Software Solutions GmbH. Seine Schwerpunkte liegen hierbei vor allem im Finanz- und Gesundheitssektor sowie KRITIS-Unternehmen. Unternehmen unterstützt er im Aufbau eines Insider-Threat-Programmes und führt in diesem Kontext auch Mitarbeiterschulungen durch.

Was ist also Ihr Fazit?

Buroh: Man könnte es so zusammenfassen, wie es Michael George, Sachbuchautor und Leiter des Cyber-Allianz-Zentrums Bayern mit seinen drei Thesen bereits in der <kes>#6/2014 beschrieben hat: „Alles ist gefährdet", „Kein Angriff ohne Interesse" und „Die Probleme von heute sind die gute alte Zeit von morgen". Gerade weil in modernen Kommunikationswegen zwischen Staat und Gesellschaft ein enormes Potenzial steckt, gleichzeitig dadurch aber immense Angriffsflächen entstehen, lohnt es sich, IT-Security als Chance zu verstehen. ■