Wichtigste Themen der nächsten 1-6 Monate

Quelle:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile&v=3

1. Informationssicherheitsaspekte müssen bei allen Projekten frühzeitig und ausreichend berücksichtigt werden

Eine möglichst große Programmvielfalt mit hoher Funktionalität, bequeme Bedienung, niedrige Anschaffungs- und Betriebskosten sowie Informationssicherheit stehen fast immer in Konkurrenz zueinander. Es empfiehlt sich aber unbedingt, Informationssicherheitsaspekte schon zu Beginn eines Projektes (z. B. bei der Anschaffung neuer Software oder bei der Planung von Geschäftsprozessen) zu berücksichtigen. Gerade neue Techniken dürfen nicht unkritisch eingesetzt werden. Unabdingbare Voraussetzung dafür ist eine klare Unterstützung der Informationssicherheitsziele durch die Leitungsebene! Später auftretende Sicherheitsmängel können unangenehme Konsequenzen zur Folge haben. Werden nachträglich Design- oder Planungsfehler offenkundig, sind Nachbesserungen oftmals unverhältnismäßig teuer oder sogar unmöglich. Der Mut, Abstriche beim Komfort zu machen oder auf eine bestimmte Funktionalität zu verzichten, kann hohe Kosten durch Sicherheitsvorfälle verhindern oder hohe Investitionen in zusätzliche Informationssicherheitsprodukte ersparen.

14. Viren-Schutzprogramme müssen flächendeckend eingesetzt werden

Aktuelle Viren-Schutzprogramme sind unverzichtbar. Schadprogramme können über Datenträger oder über Netze (Internet, Intranet) verbreitet werden. Auch für Rechner ohne Internetanschluss sind solche Schutzprogramme Pflicht!

Es empfiehlt sich, E-Mails und jegliche Kommunikation über das Internet zentral auf Viren zu untersuchen. Zusätzlich sollte jeder Computer mit einem lokalen Viren-Schutzprogramm ausgestattet sein, das ständig (resident) im Hintergrund läuft. In der Regel genügt es, nur ausführbare Dateien, Skripte, Makrodateien etc. zu überprüfen. Ein vollständiges Durchsuchen aller Dateien empfiehlt sich trotzdem in regelmäßigen Abständen (z. B. vor einer Tages- oder Monatssicherung). Bei einem festgestellten Befall durch Schadprogramme ist es immer notwendig!

Aktuelle Empfehlungen und ausführliche Hintergrundinformationen finden Sie auf der BSI-Webseite unter dem Stichwort „Schadprogramme“.

Achtung:
Selbst wenn Ihr Viren-Schutzprogramm immer auf dem neuesten Stand ist, bietet es dennoch keinen absoluten Schutz vor Schadprogrammen. Sie müssen davon ausgehen, dass Ihr System neuen Schadprogrammen zumindest solange ausgesetzt ist, bis geeignete Schadprogramm-Signaturen von den Herstellern von Schutzprogrammen zur Verfügung gestellt werden können. Gefährlich sind auch Schadprogramme, die sich über das Internet verbreiten und technisch so konstruiert sind, dass sie über eine nicht geschlossene Sicherheitslücke direkt den Rechner infizieren. Ein berühmtes Beispiel ist der Wurm „Conficker“, der eine Schwachstelle in Windows ausnutzte.

47. Alle wichtigen Daten müssen regelmäßig gesichert werden (Backup)

Für die Datensicherung (Backup) stehen zahlreiche Software- und Hardwarelösungen zur Verfügung. Es ist wichtig, dass wirklich alle relevanten Daten vom eingerichteten Backup erfasst werden. Dies stellt insbesondere bei verteilten heterogenen Umgebungen eine besondere Herausforderung dar. Auch mobile Endgeräte wie Notebooks, unvernetzte Einzelplatzrechner und auch PDAs müssen mit einbezogen werden. Es sollte regelmäßig verifiziert werden, dass das Backup auch tatsächlich funktioniert und die Daten wieder erfolgreich eingespielt werden können.

Die Backup-Medien müssen an sicherem Ort, möglichst außerhalb des Unternehmens bzw. des Dienstgebäudes, aufbewahrt werden. Der Aufbewahrungsort sollte zudem hinreichend gegen Elementarschäden wie Feuer, Wasser und Ähnliches geschützt sein.

Alle Anwender müssen wissen, welche Daten wann und wie lange gesichert werden. In der Regel werden nur bestimmte Verzeichnisse und Dateien gesichert, selten geschieht ein komplettes Backup.