IT-Sicherheit

Ungeschützt im Visier

[17.07.2015] In den meisten öffentlichen Einrichtungen reicht die IT-Sicherheit nicht aus. Das hat eine Umfrage des Digitalverbands BITKOM ergeben. Dabei sind nicht nur technische, sondern auch organisatorische, physische und personelle Maßnahmen zu beachten.

Fast die Hälfte der Behörden in Deutschland haben in den vergangenen zwei Jahren Fälle digitaler Spionage, Sabotage oder Datendiebstahl verzeichnet. Das hat eine Umfrage ergeben, die BITKOM in Auftrag gegeben hat. Laut dem Digitalverband wurden 70 Sicherheitsverantwortliche von Behörden mit zehn oder mehr Mitarbeitern befragt. Häufigstes Delikt sei mit einem Anteil von 26 Prozent Social Engineering: Mitarbeiter sollen manipuliert werden, um an bestimmte Informationen zu gelangen. Bei 23 Prozent der Behörden sind IT-Geräte mit sensiblen Daten gestohlen und bei 21 Prozent die IT-Systeme sabotiert worden. Ein Fünftel der Befragten berichte, dass sensible Dokumente entwendet wurden und bei jeder zehnten Behörde seien E-Mails ausgespäht oder Gespräche abgehört worden. „Behörden sind ein attraktives Angriffsziel für Cyber-Kriminelle und Geheimdienste“, sagt Susanne Dehmel, BITKOM-Geschäftsleiterin Vertrauen und Sicherheit. „Neben politischen Informationen sind die Angreifer auch an wirtschaftlich verwertbaren Hinweisen interessiert.“ Für den Schutz ihrer Informationen setzen alle befragten Behörden technische Maßnahmen der IT-Sicherheit ein. 94 Prozent der Einrichtungen haben Maßnahmen der organisatorischen IT-Sicherheit ergriffen und beispielsweise Verhaltensrichtlinien oder Notfallpläne ausgearbeitet. In vier von fünf Behörden gibt es laut der Umfrage physische Sicherheitsmaßnahmen, etwa um Gebäude und Einrichtungen zu schützen. Dagegen ergreife kaum ein Drittel Maßnahmen der personellen Sicherheit. „Die personelle Sicherheit wird häufig vernachlässigt. Dabei sind die eigenen Mitarbeiter die wichtigsten Garanten für den Schutz der Behörden“, erklärt Dehmel. „Die meisten Sicherheitsvorfälle werden, bewusst oder aus Unachtsamkeit, von aktuellen oder ehemaligen Beschäftigten verursacht.“ Laut der Umfrage verfügen alle befragten Behörden über Virenscanner, Firewalls und einen Passwortschutz für die verwendeten Geräte. 84 Prozent verschlüsseln ihre Netzwerkverbindungen und 59 Prozent verschlüsseln Daten auf Festplatten oder anderen Datenträgern. Nur 26 Prozent setzen auf eine Verschlüsselung ihres E-Mail-Verkehrs. Dehmel: „Wie in der Privatwirtschaft setzen Behörden noch zu selten umfassende IT-Sicherheitsmaßnahmen ein. Der Basisschutz mit Virenscannern und Firewalls reicht nicht mehr aus.“ 37 Prozent der Befragten nutzen laut BITKOM spezielle Angriffserkennungssysteme für Attacken von außen. 27 Prozent verfügen über eine Absicherung gegen Datenabfluss von innen. Nur jede zehnte Behörde setze erweiterte Verfahren zur Benutzeridentifikation ein, zum Beispiel eine Zwei-Faktor-Authentifizierung oder biometrische Merkmale. Gut ein Drittel überprüfe die eigenen Sicherheitskonzepte mithilfe so genannter Penetrationstests.

(ve)

Stichwörter: IT-Sicherheit, BITKOM, Umfrage