



## **SICHERHEITSKULTUR DER IT GEFORDERT**

Der GI-Arbeitskreis „Datenschutz und IT-Sicherheit“ fordert die Bundesregierung ausdrücklich auf, im Bereich Informationssicherheit der Bundesrepublik Deutschland nicht nur durch Strafgesetze aktiv zu werden, sondern insbesondere durch vorbeugende Maßnahmen in Unternehmen und Behörden.

Das Internet wird immer wieder als Sicherheitsrisiko für Spionage, Sabotage, Geldwäsche etc. etc. bezeichnet. Tatsächlich haben die einschlägigen strafrechtlichen Verschärfungen der EU und der Bundesregierung keinen Gewinn an Sicherheit gebracht. Flankierend müssen daher weitere Maßnahmen ergriffen werden, wie die OECD auch zu recht vorschlägt, in der Deutschland aktives Mitglied ist.

Dazu hat die OECD (Organisation for Economic Co-Operation and Development) die 'Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security' entwickelt und will damit eine groß angelegte Kampagne für mehr IT- Sicherheit starten. Diese Richtlinie wurde zwar von der Bundesregierung ausdrücklich begrüßt – aber nach wie vor nicht umgesetzt.

Die 30 vertretenen Industrienationen wollen durch die Richtlinie gemeinsam mit der Wirtschaft eine "Kultur der Sicherheit" im Internet begründen. Als Empfehlung angenommen und verabschiedet wurde das Papier vom Rat der OECD, nachdem die Sicherheitsexperten der Organisation seit dem 11. September 2001 über die Regeln beraten hatten. Die Mitgliedsstaaten der OECD sind aufgefordert, die Richtlinien unter Regierungsstellen, Unternehmen, Behörden, Organisationen und individuellen Anwendern zu verbreiten. Sicherheitsfragen sollen auf allen Regierungs- und Industrieebenen höchste Priorität erhalten.

Der Arbeitskreis fordert daher die Bundesregierung zu folgenden Aktivitäten auf – an denen sich die Gesellschaft für Informatik (GI) auch gern beteiligt:

1. Intensive Sensibilisierung aller Anwender durch unverzügliche Umsetzung der OECD Richtlinie in Deutschland. U.a. durch Übersetzung der Richtlinie und Publikation und Verteilung durch Ministerien und nachgeordnete Behörden (auch über das Internet).
2. Überprüfung der einschlägigen Gesetzeslage (Internet- und Cybercrime) nach dieser Sensibilisierungsphase sowie des Zugangskontrolldiensteschutz-Gesetzes (ZKDSG) und des Bundesdatenschutzgesetzes auf Angemessenheit – auf ausreichenden Schutz der Bürger, Unternehmen und Behörden.
3. Anweisung an die Bundesbehörden zur Umsetzung der Richtlinie bis zum Jahresende 2003 und Drängen auf Umsetzung in den Unternehmen (Selbstverpflichtung).

# STATEMENT DES GI-ARBEITSKREISES

## „DATENSCHUTZ UND IT-SICHERHEIT



4. Hinwirken darauf, dass Sicherheit zum integralen Bestandteil im Design und in der Anwendung aller Netzwerk- und IT-Systeme wird. Sofern diese Selbstbindung nicht greift, müssten weitergehende gesetzliche Vorschriften überlegt werden.

Insbesondere fordert die OECD die Mitgliedsstaaten auf:

Auf der Basis der Richtlinien neue nationale Sicherheitsstrategien, -taktiken und Maßnahmen zu formulieren und sie in Unternehmen und Behörden durchzusetzen. Die OECD-Regierungen und alle Anwender wie Unternehmen und Behörden sind gleichermaßen aufgefordert eigenverantwortlich zur Minderung der Sicherheitsrisiken beizutragen.

Das Richtlinienpapier hat die "Arbeitsgruppe zu Informationssicherheit und Datenschutz" des Wirtschaftsverbunds der 30 wichtigsten Industrienationen erarbeitet. Das Gremium will damit den Schutz der kritischen Infrastrukturen nach dem 11. September stärken, das Thema Sicherheit ins Bewusstsein aller Beteiligten bringen und den Informationsfluss über Schutzmethoden und ihre Implementierung verbessern. Die Mitgliedsstaaten werden aufgefordert, die Richtlinien unter Regierungsstellen, Unternehmen, Organisationen und individuellen Nutzern zu verbreiten.

Sicherheit soll zum integralen Bestandteil im Design und in der Anwendung aller Netzwerke und informationstechnischen Systeme werden. Sicherheitsfragen sollen auf allen Regierungs- und Industrieebenen höchste Priorität erhalten. Die Endanwender werden zudem aufgefordert, stärker als bisher bei der Auswahl und der Konfiguration von Produkten auf Sicherheitsfaktoren zu achten. Nur so könne Druck auf die Hersteller von Soft- und Hardware ausgeübt werden, bei ihren Produkten und Dienstleistungen Fragen der Sicherheit und der Verlässlichkeit in den Vordergrund zu stellen.

Die Prinzipien der Sicherheitsrichtlinie beziehen sich auf Punkte wie Sensibilisierung, die Festlegung von Verantwortlichkeiten, die rasche Reaktion auf Sicherheitspannen und die Verbreitung einer Sicherheitsethik. Die Adressaten der Sicherheitsrichtlinie werden angehalten, ihre internen und externen Arbeitsumgebungen einer permanenten Risikoanalyse zu unterziehen, um Hackereinbrüche vorzubeugen. Dabei sollen Schlüsselfaktoren wie Technologie, das physikalische und menschliche Umfeld sowie Verhaltensregeln angesichts der sich ständig wandelnden Bedrohungen aus dem Cyberspace immer wieder aufs Neue überprüft werden.

Die Endanwender werden zudem aufgefordert, stärker als bisher bei der Auswahl und der Konfiguration von Produkten auf Sicherheitsfaktoren zu achten. Nur so könne Druck auf die Hersteller von Soft- und Hardware ausgeübt werden, bei ihren Produkten und Dienstleistungen Fragen der Sicherheit und der Verlässlichkeit in den Vordergrund zu stellen. Im Detail fordert die Richtlinie:

# STATEMENT DES GI-ARBEITSKREISES

## „DATENSCHUTZ UND IT-SICHERHEIT



- 1 Sensibilisierung (Awareness)**

Alle Anwender in Unternehmen und Behörden müssen die möglichen Sicherheitsrisiken und die grundsätzlichen Schwachstellen in Hardware und Software sowie die Möglichkeiten der Verbesserung der Sicherheit bewusst machen.
- 2 Verantwortlichkeit (Responsibility)**

Anwender tragen die Verantwortung für die Sicherheit ihrer IT-Systeme und können für die von ihnen ausgehenden Gefahren haftbar sein.
- 3 Maßnahmen (Response)**

Alle Beteiligten (Anwender, Hersteller, Service-Provider) sollen rechtzeitig und kooperativ sicherheitsrelevanten Schwachstellen und Sicherheitsverletzungen vorbeugen und entdeckte Schwachstellen unverzüglich beheben und veröffentlichen.
- 4 Ethik (Ethics)**

Die berechtigten Interessen anderer Anwender müssen respektiert werden.
- 5 Demokratie (Democracy)**

Sicherheitsmaßnahmen dürfen die Werte demokratischer Gesellschaften nicht verletzen.
- 6 Risikomanagement (Risk Assessment)**

Anwender sind zur Risikobewertung und zum Risikomanagement verpflichtet.
- 7 Sicherheit ist eine Schlüsseltechnologie (Security Design and Implementation)**

Anwender und Hersteller müssen Informationssicherheit als grundlegendes Element von IT-Systemen und Netzwerken verstehen.
- 8 Sicherheits-Management (Security Management)**

Die Teilnehmer müssen ein angemessenes Sicherheits-Management betreiben.
- 9 Kontrolle (Reassessment)**

Alle Beteiligten müssen die praktizierte Sicherheit der Systeme und Netzwerke ständig überprüfen und den aktuellen Erfordernissen anpassen.

---

---

Die **Gesellschaft für Informatik e.V. (GI)** wurde 1969 in Bonn mit dem Ziel gegründet, die Informatik zu fördern. Sie verfolgt ausschließlich gemeinnützige Zwecke. Die Mitglieder der GI kommen aus Wissenschaft, Wirtschaft, Lehre und Forschung. Derzeit hat die GI rund 24.000 Mitglieder und ist damit die größte Vertretung von Informatikerinnen und Informatikern im deutschsprachigen Raum.

<http://www.gi-ev.de>