OECD Richtlinien
für die Sicherheit von Informationssystemen
und -Netzen:

Auf dem Weg zu einer Sicherheitskultur

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT
ORGANISATION FÜR WIRTSCHAFTLICHE ZUSAMMENARBEIT UND ENTWICKLUNG

Originally published by the OECD in English and in French under the titles:

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security

Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information: Vers une culture de la sécurité

For the German edition

Published by arrangement with the OECD, Paris.

ORGANISATION FÜR WIRTSCHAFTLICHE ZUSAMMENARBEIT UND ENTWICKLUNG

Gemäß Artikel 1 des in Paris am 14. Dezember 1960 unterzeichneten und am 30. September 1961 in Kraft getretenen Übereinkommens über die Organisation für Wirtschaftliche Zusammenarbeit und Entwicklung (OECD) ist es das Ziel dieser Organisation, eine Politik zu fördern, die darauf gerichtet ist,

- in den Mitgliedstaaten unter Wahrung der finanziellen Stabilität eine optimale Wirtschaftsentwicklung und Beschäftigung sowie einen steigenden Lebensstandard zu erreichen und dadurch zur Entwicklung der Weltwirtschaft beizutragen,
- in den Mitglied- und Nichtmitgliedstaaten, die in wirtschaftlicher Entwicklung begriffen sind, zu einem gesunden wirtschaftlichen Wachstum beizutragen, und
- im Einklang mit internationalen Verpflichtungen auf multilateraler und nichtdiskriminierender Grundlage zur Ausweitung des Welthandels beizutragen.

Die ursprünglichen Mitgliedstaaten der OECD sind Belgien, Dänemark, Deutschland, Frankreich, Griechenland, Irland, Island, Italien, Kanada, Luxemburg, Niederlande, Norwegen, Österreich, Portugal, Schweden, Schweiz, Spanien, Türkei, Vereinigtes Königreich und Vereinigte Staaten. Die folgenden Staaten wurden später durch Beitritt zu den in Klammern angegebenen Daten Mitglieder: Japan (28. April 1964), Finnland (28. Januar 1969), Australien (7. Juni 1971), Neuseeland (29. Mai 1973), Mexiko (18. Mai 1994), Tschechische Republik (21. Dezember 1995), Ungarn (7. Mai 1996), Polen (22. November 1996), Korea (12. Dezember 1996) und die Slowakische Republik (14. Dezember 2000).
Die Kommission der Europäischen Gemeinschaften beteiligt sich an der Arbeit der OECD (Artikel 13 des Übereinkommens der OECD).

VORWORT

Die vorliegenden *OECD Richtlinien für die Sicherheit von Informationssystemen und -Netzen: Auf dem Weg zu einer Sicherheitskultur* wurden vom Rat der OECD auf seiner 1037. Sitzung am 25. Juli 2002 in Form einer Empfehlung angenommen.

INHALTSVERZEICHNIS

RICHTLINIEN FÜR DIE SICHERHEIT VON INFORMATIONSSYSTEMEN UND -NETZEN

AUF DEM WEG ZU EINER SICHERHEITSKULTUR

VORWORT

Die Nutzung von Informationssystemen und -Netzen sowie das gesamte Umfeld der Informationstechnologie haben sich seit 1992, als die OECD zum ersten Mal die *Richtlinien für die Sicherheit von Informationssystemen* verabschiedete, grundlegend verändert. Dieser anhaltende Wandel bietet wesentliche Vorteile, macht es aber auch notwendig, dass Regierungen, Unternehmen, andere Organisationen und Einzelnutzer, die Informationssysteme und -Netze entwickeln, besitzen, anbieten, betreiben, betreuen und anwenden ("die Beteiligten"), der Sicherheit ein größeres Gewicht verleihen.

Immer leistungsfähigere Personalcomputer, konvergierende Technologien und die weite Verbreitung des Internets haben bescheidene Einzelplatzsysteme in vorwiegend geschlossenen Netzen ersetzt. Heutzutage sind Beteiligte immer öfter zusammengeschaltet, und die Verbindungen sind grenzüberschreitend. Darüber hinaus unterstützt das Internet wichtige Infrastrukturen wie Energie, Transport und Finanzen und spielt eine wesentliche Rolle dabei, wie Unternehmen ihre Geschäfte machen, wie Regierungen Bürgern und Unternehmen Dienste anbieten und wie einzelne Bürger miteinander kommunizieren und Informationen austauschen. Das Wesen und die Art der Technologien, die die Kommunikations- und Informationsinfrastruktur ausmachen, haben sich ebenfalls erheblich gewandelt. Die Anzahl und Art der Infrastrukturzugangseinrichtungen haben sich vervielfacht und schließen nun feste, schnurlose und mobile Einrichtungen ein, und ein wachsender Prozentsatz des Zugangs erfolgt im Rahmen von "always-on"-Verbindungen. Folglich haben Art, Umfang und Sensibilität der ausgetauschten Informationen wesentlich zugenommen.

Aufgrund der zunehmenden Zusammenschaltbarkeit sind Informationssysteme und -Netze heutzutage einer größeren Anzahl und Bandbreite von Gefahren und Schwachstellen ausgesetzt. Daraus ergeben sich neue Sicherheitsaspekte. Deshalb richten sich diese Richtlinien an alle Beteiligten der neuen Informationsgesellschaft und legen die Notwendigkeit eines größeren Bewusstseins von und Verständnisses für Sicherheitsaspekte sowie die Notwendigkeit der Entwicklung einer "Sicherheitskultur" nahe.

I. AUF DEM WEG ZU EINER SICHERHEITSKULTUR

Diese Richtlinien sind die Antwort auf ein sich stets wandelndes Sicherheitsumfeld, indem sie die Entwicklung einer Sicherheitskultur fördern – das bedeutet eine Konzentration auf Sicherheit bei der Entwicklung von Informationssystemen und -Netzen sowie die Annahme neuer Denk- und Verhaltensmuster bei der Anwendung und der Kommunikation innerhalb von Informationssystemen und -Netzen. Die Richtlinien stellen einen klaren Bruch mit einer Zeit dar, in der Sicherheit bei der Gestaltung und Anwendung von Netzen und Systemen häufig an zweiter Stelle stand. Die Beteiligten sind heutzutage zunehmend von Informationssystemen, -Netzen und zugehörigen Diensten abhängig, und diese müssen alle zuverlässig und sicher sein. Effektive Sicherheit ist nur mit einem Ansatz gewährleistet, der den Interessen aller Beteiligten sowie dem Wesen der Systeme, Netze und zugehörigen Dienste gebührend Rechnung trägt.

Jeder Beteiligte spielt bei der Gewährleistung von Sicherheit eine wichtige Rolle. Beteiligte sollten sich ihren Rollen entsprechend der maßgeblichen Sicherheitsrisiken und Vorsichtsmaßnahmen bewusst sein, Verantwortung übernehmen und Maßnahmen ergreifen, um die Sicherheit von Informationssystemen und -Netzen zu erhöhen.

Die Förderung einer Sicherheitskultur erfordert sowohl Führung als auch eine umfassende Beteiligung und sollte zu einem höheren Stellenwert von Sicherheitsplanung und -management sowie Verständnis für die Notwendigkeit der Sicherheit unter allen Beteiligten führen. Sicherheitsfragen sollten auf allen Regierungs- und Unternehmensebenen und von allen Beteiligten erörtert und verantwortlich behandelt werden. Diese Richtlinien stellen eine Arbeitsgrundlage auf dem Weg zu einer Sicherheitskultur in allen Bereichen der Gesellschaft dar. Die Beteiligten werden dadurch Sicherheit in die Gestaltung und Anwendung aller Informationssysteme und -Netze einbeziehen können. Die Richtlinien schlagen vor, dass alle Beteiligten eine Sicherheitskultur beschließen und fördern, die ihr Denken, ihre Einschätzung und ihr Handeln bezüglich der Aktivitäten im Zusammenhang mit Informationssystemen und -Netzen bestimmt.

II. ZIELE

Ziel dieser Richtlinien ist es:

- eine Sicherheitskultur bei allen Beteiligten als Mittel zum Schutz von Informationssystemen und -Netzen zu fördern;
- das Bewusstsein zu schaffen für die Risiken für Informationssysteme und -Netze, die vorhandenen Strategien, Praktiken, Maßnahmen und Methoden zur Bekämpfung dieser Risiken und die Notwendigkeit, diese zu beschließen und umzusetzen;

- größeres Vertrauen bei allen Beteiligten in Informationssysteme und -Netze sowie in die Art und Weise, wie sie angeboten und genutzt werden, zu schaffen;
- einen allgemeinen Bezugsrahmen zu schaffen, der den Beteiligten dabei behilflich ist, Sicherheitsaspekte zu verstehen und moralische Werte bei der Entwicklung und Umsetzung kohärenter Strategien, Praktiken, Maßnahmen und Methoden für die Sicherheit von Informationssystemen und -Netzen zu respektieren;
- Kooperation und gegebenenfalls Informationsaustausch unter allen Beteiligten bei der Entwicklung und Umsetzung von Sicherheitsstrategien, -praktiken, -maßnahmen und -methoden zu fördern;
- die Berücksichtigung von Sicherheit als ein wichtiges Ziel unter den an der Entwicklung und Umsetzung von Normen Beteiligten zu fördern.

III. GRUNDSÄTZE

Die folgenden neun Grundsätze ergänzen sich und sollten als Einheit betrachtet werden. Sie beziehen sich auf Beteiligte auf allen Ebenen einschließlich der politischen und betrieblichen Bereiche. Gemäß diesen Richtlinien unterscheidet sich die Verantwortung der Beteiligten entsprechend ihren Rollen. Bewusstsein, Bildung, Informationsaustausch und Ausbildung verhelfen allen Beteiligten zu einem besseren Sicherheitsverständnis und zu besseren Sicherheitsstrategien. Anstrengungen zur Verbesserung der Sicherheit von Informationssystemen und -Netzen sollten mit den Werten einer demokratischen Gesellschaft vereinbar sein, insbesondere mit der Notwendigkeit eines offenen und freien Informationsflusses und mit der Achtung der Privatsphäre.[1]

[1] Neben diesen Sicherheitsrichtlinien hat die OECD zusätzliche Empfehlungen hinsichtlich weiterer für die globale Informationsgesellschaft relevanter Aspekte entwickelt. Sie beziehen sich auf die Privatsphäre (die OECD-Richtlinien bezüglich des Schutzes der Privatsphäre und des grenzüberschreitenden Flusses personenbezogener Daten von 1980) und Kryptographie (die OECD-Richtlinien für Kryptographie-Politik von 1997). Diese Sicherheitsrichtlinien sollten im Zusammenhang mit ihnen betrachtet werden.

1) Bewusstsein

Die Beteiligten sollten sich der Notwendigkeit der Sicherheit von Informationssystemen und -Netzen und ihres Beitrages zur Erhöhung der Sicherheit bewusst sein.

Das Bewusstsein von Risiken und vorhandenen Schutzvorkehrungen ist der erste Schritt zum Schutz der Sicherheit von Informationssystemen und -Netzen. Informationssysteme und -Netze können sowohl nationalen als auch internationalen Risiken ausgesetzt sein. Die Beteiligten sollten verstehen, dass Sicherheitsmängel zu erheblichem Schaden an von ihnen kontrollierten Systemen und Netzen führen können. Darüber hinaus sollten sie sich des potenziellen Schadens für andere angesichts von Zusammenschaltungen und Abhängigkeiten bewusst sein. Die Beteiligten sollten sich der Konfiguration ihres Systems und vorhandener aktueller Versionen, seiner Rolle innerhalb von Netzen, vorbildlichen Beispielen, die sie zur Erhöhung der Sicherheit umsetzen können, sowie der Bedürfnisse anderer Beteiligter bewusst sein.

2) Verantwortung

Alle Beteiligten sind für die Sicherheit von Informationssystemen und -Netzen verantwortlich.

Die Beteiligten sind von zusammengeschalteten lokalen und globalen Informationssystemen und -Netzen abhängig und sollten sich ihrer Verantwortung für die Sicherheit dieser Informationssysteme und -Netze bewusst sein. Sie sollten in einer ihrer jeweiligen Rolle entsprechenden Form zur Rechenschaft gezogen werden können. Die Beteiligten sollten ihre eigenen Strategien, Praktiken, Maßnahmen und Methoden regelmäßig überprüfen und beurteilen, ob diese ihrem Umfeld angemessen sind. Diejenigen, die Produkte und Dienste entwickeln, gestalten und anbieten, sollten sich mit System- und Netzsicherheit beschäftigen und entsprechende Informationen einschließlich aktueller Versionen rechtzeitig verbreiten, so dass Anwender die Sicherheitsfunktionalität von Produkten und Diensten sowie ihre Verantwortung bezüglich Sicherheit besser verstehen können.

3) Reaktion

Die Beteiligten sollten rechtzeitig und in einer kooperativen Art und Weise handeln, um Zwischenfälle, die die Sicherheit gefährden, zu verhindern, aufzudecken und darauf zu reagieren.

Angesichts der Zusammenschaltbarkeit von Informationssystemen und -Netzen und von möglichem, schnell angerichtetem und weit reichendem Schaden sollten die Beteiligten hinsichtlich Sicherheitszwischenfälle rechtzeitig und in einer kooperativen Art und Weise handeln. Sie sollten gegebenenfalls Informationen über Gefahren und Schwachstellen austauschen und

Methoden der schnellen und effektiven Kooperation zur Vermeidung und Aufdeckung von Sicherheitszwischenfällen sowie Reaktion auf Sicherheitszwischenfälle umsetzen. Dazu gehören gegebenenfalls grenzüberschreitender Informationsaustausch und grenzüberschreitende Kooperation.

4) Moral

Die Beteiligten sollten die legitimen Interessen anderer respektieren.

Angesichts der Verbreitung von Informationssystemen und -Netzen in unseren Gesellschaften müssen die Beteiligten erkennen, dass ihr Handeln oder das Unterlassen ihres Handelns anderen schaden kann. Moralisches Verhalten ist daher entscheidend, und die Beteiligten sollten anstreben, vorbildliches Verhalten zu entwickeln und umzusetzen und Verhalten zu fördern, das Sicherheitsbedürfnisse anerkennt und die legitimen Interessen anderer respektiert.

5) Demokratie

Die Sicherheit von Informationssystemen und -Netzen sollte mit den wesentlichen Werten einer demokratischen Gesellschaft vereinbar sein.

Sicherheit sollte in einer Art und Weise umgesetzt werden, die mit den anerkannten Werten demokratischer Gesellschaften vereinbar ist; zu diesen zählen ungehinderter Gedanken- und Ideenaustausch, ungehinderter Informationsfluss, die Vertraulichkeit von Informationen und Mitteilungen, geeigneter Schutz personenbezogener Daten sowie Offenheit und Transparenz.

6) Risikoeinschätzung

Die Beteiligten sollten Risikoeinschätzungen durchführen.

Im Rahmen von Risikoeinschätzungen werden Gefahren und Schwachstellen erkannt; sie sollten ausreichend breit gefächert sein, um wesentliche interne und externe Faktoren wie Technologie, physische und humane Faktoren, Strategien und Dienste seitens Dritter mit Sicherheitsrelevanz einzuschließen. Risikoeinschätzungen helfen bei der Bestimmung des akzeptablen Risikograd es und bei der Wahl geeigneter Kontrollmechanismen, um die Gefahr potenziellen Schadens an Informationssystemen und -Netzen angesichts des Wesens und der Bedeutung der zu schützenden Information in Grenzen zu halten. In Anbetracht der wachsenden Zusammenschaltbarkeit von Informationssystemen sollten Risikoeinschätzungen die Erwägung von potenziellem Schaden, der von anderen ausgehen oder anderen entstehen kann, umfassen.

7) Sicherheitsgestaltung und -umsetzung

Die Beteiligten sollten Sicherheit als wesentlichen Bestandteil von Informationssystemen und -Netzen aufnehmen.

Systeme, Netze und Strategien müssen vernünftig gestaltet, umgesetzt und koordiniert werden, um die Sicherheit zu optimieren. Ein wichtiger, wenn auch nicht der einzige Schwerpunkt dieser Anstrengung ist die Gestaltung und Annahme geeigneter Schutzvorkehrungen und Lösungen zur Vermeidung bzw. Begrenzung potenziellen Schadens durch bekannte Gefahren und Schwachstellen. Sowohl technische als auch nicht-technische Schutzvorkehrungen und Lösungen sind notwendig und sollten in einem angemessenen Verhältnis zum Wert der Informationen auf den Systemen und Netzen der Organisation stehen. Sicherheit sollte ein wesentliches Element aller Produkte, Dienste, Systeme und Netze und fester Bestandteil von Systemgestaltung und -aufbau sein. Für Endnutzer besteht Sicherheitsgestaltung und -umsetzung weitgehend darin, Produkte und Dienste für ihr System auszuwählen und zusammenzustellen.

8) Sicherheitsmanagement

Die Beteiligten sollten ein umfassendes Sicherheitsmanagement-Konzept entwickeln.

Sicherheitsmanagement sollte auf Risikoeinschätzung basieren und dynamisch sein und alle Bereiche der Aktivitäten der Beteiligten und alle Aspekte ihrer Tätigkeit umfassen. Es sollte präventive Maßnahmen bezüglich Gefahren einschließen und sich mit den Aspekten Vermeidung und Aufdeckung von Zwischenfällen und Reaktion auf Zwischenfälle, Systemwiederherstellung, laufende Wartung, Überprüfung und Revision beschäftigen. Sicherheitsstrategien, -praktiken, -maßnahmen und -methoden für Informationssysteme und -Netze sollten koordiniert werden, um ein kohärentes Sicherheitssystem zu bilden. Die Anforderungen des Sicherheitsmanagements hängen vom Beteiligungsgrad und von der Rolle des Beteiligten, vom jeweiligen Risiko sowie von den Systemanforderungen ab.

9) Neufestlegung

Die Beteiligten sollten die Sicherheit von Informationssystemen und -Netzen überprüfen und neu festlegen und Sicherheitsstrategien, -praktiken, -maßnahmen und -methoden entsprechend ändern.

Ständig werden neue, sich wandelnde Gefahren und Schwachstellen aufgedeckt. Die Beteiligten sollten alle diese neuen Gefahren betreffenden Sicherheitsaspekte kontinuierlich überprüfen, neu festlegen und ändern.

EMPFEHLUNG DES RATES HINSICHTLICH RICHTLINIEN FÜR DIE SICHERHEIT VON INFORMATIONSSYSTEMEN UND -NETZEN

AUF DEM WEG ZU EINER SICHERHEITSKULTUR

DER RAT,

eingedenk der Konvention über die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung vom 14. Dezember 1960, insbesondere der Artikel 1 b), 1 c), 3 a) und 5 b);

eingedenk der Empfehlung des Rates hinsichtlich der Richtlinien bezüglich des Schutzes der Privatsphäre und des grenzüberschreitenden Flusses personenbezogener Daten vom 23. September 1980 [R(80)58/endgültig)];

eingedenk der Erklärung über grenzüberschreitenden Datenfluss, die von den Regierungen von OECD-Mitgliedstaaten am 11. April 1985 angenommen wurde [Anhang zu R(85)139];

eingedenk der Empfehlung des Rates hinsichtlich der Richtlinien für Kryptographie-Politik vom 27. März 1997 [R(97)62/endgültig];

eingedenk der Ministererklärung über den Schutz der Privatsphäre auf globalen Netzen vom 7. - 9. Dezember 1998 [Anhang zu R(98)177/endgültig];

eingedenk der Ministererklärung über die Authentifizierung für elektronischen Geschäftsverkehr vom 7. - 9. Dezember 1998 [Anhang zu R(98)177/endgültig];

in Anerkennung, dass die Nutzung und der Wert von Informationssystemen und -Netzen für Regierungen, Unternehmen, andere Organisationen und Einzelnutzer zunehmen;

in Anerkennung, dass die zunehmende Bedeutung von Informationssystemen und -Netzen und die wachsende Abhängigkeit von ihnen für stabile und effiziente Volkswirtschaften und internationalen Handel sowie im sozialen, kulturellen und politischen Leben besondere Anstrengungen notwendig machen, diese zu schützen und das Vertrauen in sie zu fördern;

in Anerkennung, dass Informationssysteme und -Netze und ihre weltweite Verbreitung mit neuen und wachsenden Risiken einhergehen;

in Anerkennung, dass Daten und Informationen, die auf Informationssystemen und -Netzen gespeichert und mittels dieser übertragen werden, Gegenstand von Gefahren verschiedener Art einschließlich unbefugtem Zugriff, unbefugter Nutzung, Missbrauch, Manipulation, unbefugter Code-Übermittlung, Diensteverweigerung oder Zerstörung sind und geeignete Schutzvorkehrungen erfordern;

in Anerkennung, dass es notwendig ist, das Bewusstsein für die Gefahren für Informationssysteme und -Netze sowie für Strategien, Praktiken, Maßnahmen und Methoden, die zur Bekämpfung dieser Gefahren zur Verfügung stehen, zu schaffen und angemessenes Verhalten als einen wesentlichen Schritt zur Entwicklung einer Sicherheitskultur zu fördern;

in Anerkennung, dass es notwendig ist, die bestehenden Strategien, Praktiken, Maßnahmen und Methoden zu überprüfen, um dazu beizutragen sicherzustellen, dass sie den neuen Herausforderungen angesichts der Gefahren für Informationssysteme und -Netze gewachsen sind;

in Anerkennung, dass ein gemeinsames Interesse daran besteht, die Sicherheit von Informationssystemen und -Netzen durch eine Sicherheitskultur zu erhöhen, die die internationale Koordination und Kooperation fördert, um den Herausforderungen angesichts des potenziellen Schadens infolge von Sicherheitsmängeln für Volkswirtschaften, den internationalen Handel und die Teilhabe am sozialen, kulturellen und politischen Leben gewachsen zu sein;

und darüber hinaus in Anerkennung, dass die im Anhang zu dieser Empfehlung genannten *Richtlinien für die Sicherheit von Informationssystemen und -Netzen: Auf dem Weg zu einer Sicherheitskultur* freiwilliger Natur sind und die souveränen Rechte der Nationen nicht berühren;

und in Anerkennung, dass diese Richtlinien nicht den Eindruck erwecken sollen, dass es eine einzige Lösung für Sicherheit gibt, oder nahe legen sollen, welche Strategien, Praktiken, Maßnahmen und Methoden für eine bestimmte Situation geeignet sind, sondern dass sie vielmehr einen Rahmen von Grundsätzen darstellen sollen, um ein besseres Verständnis dafür zu schaffen, wie die Beteiligten sowohl von der Entwicklung einer Sicherheitskultur profitieren als auch dazu beitragen können;

EMPFIEHLT diese *Richtlinien für die Sicherheit der Informationssysteme und -Netze: Auf dem Weg zu einer Sicherheitskultur* Regierungen, Unternehmen, anderen Organisationen und Einzelnutzern, die Informationssysteme und -Netze entwickeln, besitzen, anbieten, betreiben, betreuen und anwenden;

GIBT Mitgliedstaaten DIE EMPFEHLUNG,

neue Strategien, Praktiken, Maßnahmen und Methoden zu entwickeln oder bestehende zu ändern, um die *Richtlinien für die Sicherheit der Informationssysteme und -Netze: Auf dem Weg zu einer Sicherheitskultur* widerzuspiegeln und zu berücksichtigen, indem sie eine Sicherheitskultur auf der Grundlage der Richtlinien beschließen und fördern;

sich zur Umsetzung der Richtlinien auf nationaler und internationaler Ebene zu beraten, zu koordinieren und kooperieren;

die Richtlinien im öffentlichen und privaten Bereich einschließlich an Regierungen, Unternehmen, andere Organisationen und Einzelnutzer weiterzuleiten und alle Beteiligten dazu zu ermutigen, verantwortlich zu handeln und die notwendigen Maßnahmen zur Umsetzung der Richtlinien in einer ihrer jeweiligen Rolle angemessenen Art und Weise zu ergreifen;

die Richtlinien Nicht-Mitgliedstaaten rechtzeitig und in geeigneter Form zur Verfügung zu stellen;

die Richtlinien alle fünf Jahre zu überprüfen, um die internationale Kooperation bezüglich Angelegenheiten, die sich auf die Sicherheit von Informationssystemen und -Netzen beziehen, zu fördern;

WEIST den OECD-Ausschuss für Informations-, Computer- und Kommunikationspolitik AN, die Umsetzung der Richtlinien zu fördern.

Diese Empfehlung ersetzt die Empfehlung des Rates hinsichtlich Richtlinien für die Sicherheit von Informationssystemen vom 26. November 1992 [R(92)188/endgültig].

ENTSTEHUNGSGESCHICHTE

Die Sicherheitsrichtlinien wurden erstmals 1992 fertig gestellt und 1997 überprüft. Die aktuelle Überprüfung erfolgte 2001 durch die Arbeitsgruppe für Informationssicherheit und Privatsphäre (WPISP) gemäß dem Mandat des Ausschusses für Informations-, Computer- und Kommunikationspolitik (ICCP) und wurde in Folge der Tragödie vom 11. September beschleunigt.

Die redaktionellen Arbeiten erledigte eine Expertengruppe der WPISP, die am 10. und 11. Dezember 2001 in Washington, DC, am 12. und 13. Februar in Sydney und am 4. und 6. März in Paris zusammenkam. Die WPISP trat am 5.-6. März 2002, 22.-23. April 2002 und 25.-26. Juni 2002 in Paris zusammen.

Die vorliegenden *OECD-Richtlinien für die Sicherheit von Informationssystemen und -Netzen: Auf dem Weg zu einer Sicherheitskultur* wurden vom Rat der OECD auf seiner 1037. Sitzung am 25. Juli 2002 in Form einer Empfehlung angenommen.