



Informationsverarbeitung — Sicherheitstechnische Anforderungen an Webapplikationen

Information technology — Technical requirements concerning the security of web applications

Traitement de l'information — Exigences techniques de sécurité pour applications du réseau web

Medieninhaber und Hersteller

ON Österreichisches Normungsinstitut
Austrian Standards Institute
Heinestraße 38, 1020 Wien

Copyright © ON 2008. Alle Rechte vorbehalten!

Nachdruck oder Vervielfältigung, Aufnahme auf oder in sonstige Medien oder Datenträger nur mit Zustimmung des ON gestattet!
E-Mail: copyright@on-norm.at

Verkauf von in- und ausländischen Normen und Regelwerken durch
ON Österreichisches Normungsinstitut
Austrian Standards Institute
Heinestraße 38, 1020 Wien
E-Mail: sales@on-norm.at
Internet: www.on-norm.at/shop
Fax: +43 1 213 00-818
Tel.: +43 1 213 00-805

ICS 35.040; 35.100.01; 35.240.99

Ersatz für ONR 17700:2005-06

zuständig ON-Komitee ON-K 001
Informationsverarbeitung

Inhalt

Vorwort	3
1 Anwendungsbereich	4
2 Begriffe	4
3 Architektur der Webapplikation	6
4 Datenspeicherung und Datentransport	7
5 Konfigurationsdaten	7
6 Authentifizierung, Autorisierung und Sitzungen	7
6.1 Allgemeines	7
6.2 Authentifizierung	7
6.2.1 Authentifizierungsmethoden	7
6.2.2 Passwörter	7
6.3 Autorisierung	8
6.4 Sitzungen	8
6.4.1 Separierung durch Sitzungen	8
6.4.2 Qualitätskriterien für Sitzungen	8
7 Behandlung von Benutzereingaben	8
7.1 Anforderungen	8
7.2 Dateigenerierung	9
7.3 Speichermanagement	9
7.4 Einbinden von Ressourcen	9
8 Behandlung von Datenausgaben	9
9 Hintergrundsysteme	9
10 System- und Fehlermeldungen	9
11 Kryptographie	10
Literaturhinweise	11

Vorwort

Webapplikationen sind heute allgegenwärtig. Im Endkundenbereich, zwischen Geschäftspartnern und zwischen Bürger und Behörde werden vielfach Webapplikationen eingesetzt. Anwendungsbeispiele reichen von der Suche nach Informationen über Auktionen bis hin zur Produktbestellung, Internet-Banking oder der Abbildung gesamter Logistik-Ketten. Auch der Zugriff auf Applikationen des unternehmenseigenen Intranets wird immer häufiger über das Internet angeboten.

Diese rasante Entwicklung wird von den Möglichkeiten angetrieben, Geschäftsprozesse zu vereinfachen, zu beschleunigen und damit deren Produktivität zu erhöhen. Die Nutzung von Webapplikationen kann zu Kosteneinsparungen führen, Wettbewerbsvorteile schaffen und neue Geschäftsfelder eröffnen.

Im Bestreben, diese Vorteile bestmöglich zu nutzen, werden die dabei entstehenden Risiken häufig vernachlässigt. Folgende Risiken treten typischerweise bei der Entwicklung von Webapplikation auf:

- Konzepte, die sich in anderen Bereichen der Informationstechnologie bewährt haben, werden ins Web übernommen, ohne ihre Eignung und ihre Sicherheit zu hinterfragen.
- Sensible Daten und Verbindungen zu Hintergrundsystemen werden ohne zusätzliche Schutzmaßnahmen über Webapplikationen zugänglich gemacht, häufig in der fälschlichen Annahme, der erforderliche Schutz sei durch den Einsatz von netzwerkbasierter Firewall-Systemen oder Application-Level-Firewalls gegeben.
- Webapplikationen werden in den Produktivbetrieb überführt, ohne strenge Qualitätskontrollen in Bezug auf Sicherheitseigenschaften zu durchlaufen.
- Unternehmenskritische Geschäftsprozesse werden direkt in Webapplikationen abgebildet, ohne ihre Sicherheitsanforderungen zu erheben und geeignete Schutzmaßnahmen zu implementieren.

Bereits im Vorfeld der eigentlichen Entwicklung kann die Sicherheit in vielen Fällen durch optimierte Ressourcenverteilung angehoben werden. Durch das Setzen präventiver Aktionen lassen sich die folgenden Probleme vermeiden:

- Richtlinien zur sicheren Programmierung werden nicht vorgegeben oder beachtet.
- Freigabeprozesse, die vor der Produktivschaltung ein definiertes Sicherheitsniveau herstellen würden, existieren nicht.
- Schutzmaßnahmen werden zugunsten maximaler Anwenderfreundlichkeit und Kostenersparnis nicht angewandt.
- Die Sicherheit der Anwendung als Teilaspekt des Gesamtprojektes wird bei der Erstellung des Software-entwicklungsbudgets nicht eingeplant.

Der freie Zugang zum Internet macht Webapplikationen nicht nur für legitime Benutzer, sondern auch für Angreifer (Hacker) erreichbar. Das Web bietet eine Reihe von Möglichkeiten, anonym zu agieren. Das Risiko für geschickte Angreifer ist daher gering und die Hemmschwelle entsprechend niedrig. Das Web ist in vielen Fällen direkter Umsatzträger eines Unternehmens und kann daher den Geschäftserfolg massiv beeinflussen. Wegen seiner einfachen Zugangsmöglichkeiten wird das Web auch von Anwendern genutzt, die nicht die erforderlichen Kenntnisse besitzen, sich angemessen zu schützen.

Aus diesen Gründen steht die Forderung nach möglichst uneingeschränkter Nutzung im ständigen Zielkonflikt mit den Erfordernissen der Sicherheit. Ziel dieser ÖNORM ist es daher, dass das Risikopotential einer Webapplikation sowohl für Unternehmen als auch für Anwender entscheidend gesenkt wird.

Die vorliegende Ausgabe ist eine Neubearbeitung der ONR 17700:2006 und unterscheidet sich vollkommen von der bisherigen Ausgabe der ONR.

1 Anwendungsbereich

Diese ÖNORM legt Anforderungen an die Sicherheit von Webapplikationen fest. Sicherheit wird durch Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit aller von der Anwendung verarbeiteten Informationen erfüllt. Die Klassifizierung dieser Anforderungen obliegt dem Anwender dieser ÖNORM und ist schriftlich zu dokumentieren.

Diese ÖNORM bezieht sich ausschließlich auf die Webapplikation selbst. Komponenten, die zum Betrieb der Anwendung benötigt werden (zB Betriebssystem, Webserver, Netzwerkkomponenten) sowie Hintergrundsysteme (zB Datenbanken, Legacysysteme) werden nicht behandelt.

Es werden die Sicherheitsanforderungen an Webapplikationen aus einer generischen und technologieunabhängigen Sicht behandelt. Die einzelnen Anforderungen sind daher in diesem Dokument nicht auf spezifische technologische Lösungen abgebildet, wodurch ein entsprechend hoher Wissensstand beim Benutzer dieser ÖNORM Voraussetzung ist. Ergänzende Informationen können aus einschlägiger Literatur, wie zB dem OWASP Guide, bezogen werden.

Die Sicherheit der in der Webapplikation abgebildeten Prozesse sowie logische Fehler darin sind nicht Teil dieser ÖNORM, da die hier definierten Anforderungen rein technischer Natur sind.

Um bestimmen zu können, ob eine Webapplikation den Anforderungen dieser ÖNORM genügt, muss der Umfang der Webapplikation abgegrenzt und dokumentiert sowie deren Schnittstellen nach außen spezifiziert werden. Da Angriffe immer über die zur Verfügung gestellten Schnittstellen durchgeführt werden, müssen diese bekannt und ebenfalls dokumentiert sein, um die Sicherheit der Anwendung bewerten zu können.

Ist die Sicherheit der Webapplikation untrennbar mit der Konfiguration einer zugrunde liegenden Komponente verbunden, muss die relevante Konfiguration in den Anwendungsbereich mit aufgenommen werden.

2 Begriffe

Für die Anwendung dieser ÖNORM gelten die folgenden Begriffe:

2.1

Altsystem

en Legacy-System

etablierte, historisch gewachsene Anwendung

Altsysteme sind meist großrechnerbasierte Individualentwicklungen.

2.2

Authentifizierung

en Authentication

Überprüfung, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein

2.3

Authentisierung

en Authentication

Vorlage eines Nachweises eines Kommunikationspartners, dass er tatsächlich derjenige ist, der er vorgibt zu sein

2.4**Autorisierung
en Authorization**

Prüfung, ob eine Person, IT-Komponente oder Anwendung zur Durchführung einer bestimmten Aktion berechtigt ist

2.5**Benutzer**

Person oder Anwendung, die auf die Webapplikation zugreift

2.6**Benutzereingaben**

alle Daten, die vom Benutzer der Webapplikation an diese herangetragen werden (können)

2.7**Brute-Force-Methode**

Ausprobieren möglicher Fälle für die Lösung eines Problems (zB Finden des korrekten Passwortes für einen Benutzer-Account)

2.8**Entropie**

Maß für den Informationsgehalt eines Zeichens oder einer Zeichenfolge

2.9**Filter**

Verfahren und Methoden, die Daten gezielt auszuwählen oder einzuschränken und somit zu bereinigen

Das Ziel von Filtern ist es, eine Datenmenge in erwünschte und unerwünschte Daten zu trennen.

2.10**Hintergrundsystem
en Backend**

IT-Anwendung, die zur der Speicherung und Verwaltung der Daten dient

2.11**Hypertext-Übertragungsprotokoll
en Hypertext Transfer Protocol (HTTP)**

Protokoll, das zur Übertragung von Daten zwischen einem HTTP-Server und einem HTTP-Client (zB einem Browser) dient

Das Protokoll ist in RFC 2616 spezifiziert und basiert auf dem Client-Server-Prinzip. Das bedeutet, dass stets vom Client eine Anfrage gestellt wird, die vom Webserver beantwortet wird.

2.12**Interpreter-Injection**

Angriff auf Interpreter durch Manipulation von Parametern

2.13**Minimalprinzip
en Principle of least privilege**

Prinzip, dass die gewünschte Funktionalität mit den minimal notwendigen Ressourcen erreicht werden muss

Das Minimalprinzip bedeutet, dass für die Verarbeitung von Daten und die Ausführung von Operationen nur die mindestens erforderlichen Rechte verwendet werden dürfen. Zusätzlich dürfen keine Komponenten, Ressourcen und Funktionen vorhanden sein, die für die gewünschte Funktionalität der Webapplikation nicht unbedingt notwendig sind. Diese gewünschte Funktionalität muss in Form von Use-Cases dokumentiert sein.

2.14

Schwarze Listen Blacklist

Liste von Objekten, die ausdrücklich verboten sind

2.15

Sitzungen Session

Verbindung, die dazu dient, Daten über mehrere HTTP-Anfragen hinweg einem Benutzer zuordenbar zu machen

Dazu wird dem Benutzer ein eindeutiger Sitzungsidentifikator zugewiesen, der bei jeder Anfrage an den Webserver übermittelt wird. Zustandsbehaftete Webapplikationen benötigen Sitzungen.

2.16

Verschlüsselung

Vorgang, bei dem ein Klartext mit Hilfe eines kryptographischen Verfahrens in einen rückrechenbaren Geheimtext umgewandelt wird

Als entscheidend wichtige Parameter der Verschlüsselung werden hierbei ein oder auch mehrere Schlüssel verwendet.

2.17

Webapplikation

Applikation, die den Benutzern Informationen und Funktionalitäten über HTTP zur Verfügung stellt

Eine Webapplikation besteht aus einer oder mehreren der nachfolgenden Schichten:

- Präsentationsschicht (en Presentation-Layer): Schnittstelle zur Kommunikation zwischen der Webapplikation und ihren Benutzern.
- Anwendungsschicht (en Application-Layer): Enthält die Programmlogik. Die Anwendungsschicht nimmt Daten von der Präsentationsschicht entgegen und verarbeitet diese. Zusätzlich kann die Anwendungsschicht Daten der Datenschicht verwenden und bearbeiten.
- Datenschicht (en Data-Layer): Speichert die Daten in dazu geeigneten Hintergrundsystemen (zB Datenbanken, Verzeichnisdiensten oder Dateien).

2.18

Webservices

Services, die den Anwendungen Informationen und Funktionalitäten in strukturierter Form zur Verfügung stellen

Da Webservices die gleichen Protokolle wie Web-Anwendungen verwenden, sind sie hinsichtlich Sicherheitsanforderungen mit Web-Anwendungen gleichzusetzen.

2.19

Weißer Liste Whitelist

Liste von Objekten, die ausdrücklich erlaubt sind

3 Architektur der Webapplikation

Die Webapplikation muss dem Minimalprinzip entsprechen. Sofern die Anwendung Eingaben oder Ausgaben verarbeitet, sind Möglichkeiten zur Implementierung von Filtermechanismen vorzusehen.

4 Datenspeicherung und Datentransport

Die Webapplikation muss eine Möglichkeit zum verschlüsselten Speichern von vertraulichen Informationen und zum sicheren Transport dieser zwischen den Schichten bieten. Die Kommunikation der äußersten Schicht (Präsentationsschicht) über nicht vertrauenswürdige Kanäle muss für vertrauliche Informationen verschlüsselt erfolgen.

5 Konfigurationsdaten

Für Konfigurationsdaten gelten folgende Anforderungen:

- Konfigurationsdaten müssen so geschützt werden, dass sie nicht unbefugt ausgelesen oder verändert werden können.
- Standardeinstellungen müssen so definiert sein, dass keine Sicherheitsrisiken von ihnen ausgehen.
- Konfigurationen müssen dem Minimalprinzip entsprechen.

6 Authentifizierung, Autorisierung und Sitzungen

6.1 Allgemeines

Die Webapplikation muss in Abhängigkeit von den vom Betreiber zu definierenden Sicherheitsanforderungen geeignete Authentifizierungsmethoden umsetzen.

Wenn die Notwendigkeit besteht, Benutzer voneinander eindeutig zu unterscheiden, muss die Webapplikation die Authentifizierung und Autorisierung von Benutzern ermöglichen.

Verfügt die Webapplikation über Mechanismen, um Benutzer zu authentifizieren und zu autorisieren, oder kommen Sitzungen zum Einsatz, müssen die in den folgenden Abschnitten definierten Anforderungen umgesetzt werden.

6.2 Authentifizierung

Die Webapplikation muss bei der Authentifizierung sicherstellen, dass jeder Benutzer mit Hilfe einer vertraulichen Komponente eindeutig identifiziert werden kann.

6.2.1 Authentifizierungsmethoden

Die Authentifizierungsmethoden müssen von der Webapplikation selbst oder durch Schnittstellen zu einem externen Berechtigungssystem implementiert werden.

6.2.2 Passwörter

Bei Verwendung von Passwörtern für die Benutzerauthentifizierung müssen folgende Anforderungen erfüllt werden:

- Bei der Übertragung und Ablage von Passwörtern muss deren Geheimhaltung durch geeignete Verfahren (zB Verschlüsselung, Verwendung von kryptographischen Einwegfunktionen) gewährleistet sein.
- Passwörter dürfen nur in der Datenschicht hinterlegt werden.
- Das Erraten von Passwörtern mittels Brute-Force-Methoden muss durch geeignete Verfahren mit definierbarer Wahrscheinlichkeit unterbunden werden.
- Die Webapplikation muss in der Lage sein, die Umsetzung einer vorgegebenen Passwort-Policy zu erzwingen.

6.3 Autorisierung

Webapplikationen dürfen dem Benutzer nur die minimalen, zur Ausführung der erforderlichen Funktionen benötigten Rechte zuweisen. Alle nicht öffentlich zugänglichen Informationen bzw. Objekte dürfen nur den dazu berechtigten Benutzern zur Verfügung stehen. Die Autorisierung muss serverseitig erfolgen und darf nicht auf den Client ausgelagert werden.

6.4 Sitzungen

Bei zustandsbehafteten Webapplikationen müssen Sitzungen verwendet werden. Dabei sind die Anforderungen gemäß 6.4.1 und 6.4.2 zu beachten.

6.4.1 Separierung durch Sitzungen

Wenn Sitzungen verwendet werden, um Daten einem Benutzer innerhalb eines Besuchs der Webapplikation eindeutig zuzuordnen, gelten folgende Anforderungen:

- Um die Sitzungsdaten einem Benutzer eindeutig zuordnen zu können, muss jedem Benutzer nach erfolgreicher Authentifizierung ein Sitzungsidentifikator zugewiesen werden.
- Applikationsinterne Daten, die einem Benutzer eindeutig zugeordnet werden, müssen am Server verwaltet und über die Sitzung angesprochen werden. Sie dürfen nicht vom Client direkt manipulierbar sein.

6.4.2 Qualitätskriterien für Sitzungen

Es gelten folgenden Anforderungen:

- Die Webapplikation muss eine Funktion zur Verfügung stellen, mit der ein Benutzer seine aktuelle Sitzung beenden kann.
- Die Webapplikation muss Sitzungsidentifikatoren mit einer ausreichend hohen Entropie und Zufälligkeit erzeugen, sodass erfolgreiche Brute-Force-Angriffe während einer bestehenden Sitzung mit am Markt verfügbaren Mitteln praktisch ausgeschlossen werden können.
- Die Webapplikation muss nach einer definierbaren Zeitspanne an Inaktivität eines Benutzers die Sitzung beenden.
- Wird ein Benutzer mit Hilfe der Sitzung authentifiziert, darf der Sitzungsidentifikator nur über verschlüsselte Kanäle übertragen werden.
- Sitzungsidentifikatoren dürfen nicht in der URL übertragen werden.

7 Behandlung von Benutzereingaben

7.1 Anforderungen

Für Benutzereingaben gelten folgende Anforderungen:

- Benutzereingaben sind einer Eingabeüberprüfung zu unterziehen. Dabei muss die Dateneingabe hinsichtlich Inhalt, Plausibilität, gültigen Wertebereich, erlaubten Zeichen, Länge und Typ überprüft werden.
- Bei Verwendung von Benutzereingaben beim Zugriff auf Hintergrundsysteme, bei Dateizugriffen, beim Ausführen von Betriebssystem-Kommandos und beim Zugriff auf andere Schnittstellen müssen Filter, Kodierungen oder Methoden eingesetzt werden, die keine Steuerzeichen verarbeiten. Diese müssen verhindern, dass durch Interpreter-Injection die Vertraulichkeit, Integrität oder Verfügbarkeit beeinträchtigt werden kann.
- Bei der Validierung der Benutzereingaben müssen alle Kodierungen berücksichtigt werden, die es ermöglichen, Angriffsvektoren an die Webapplikation heranzutragen.
- Die Überprüfung der Daten auf ihre Gültigkeit muss serverseitig erfolgen.

7.2 Dateigenerierung

Sollte die Webapplikation serverseitig Dateien generieren, gelten hierfür folgende Anforderungen:

- Der Dateityp der am Server zu speichernden Datei muss dem erwarteten Dateityp entsprechen.
- Die Dateiendung der generierten Datei muss überprüft und eingeschränkt werden.
- Die maximale Größe einer zu generierenden Datei muss definiert werden.
- In Bezug auf die Dateigenerierung muss das Minimalprinzip erfüllt werden. Dateien dürfen nur generiert werden, sofern es für die korrekte Funktionalität der Anwendung notwendig ist.

7.3 Speichermanagement

Benutzereingaben dürfen die Integrität des Hauptspeichers nicht verletzen. Bei der Übergabe von Benutzereingaben an einen systemnahen Code in der Webapplikation müssen Filter gegen Speichermanagement-Fehler vorhanden sein.

7.4 Einbinden von Ressourcen

Für die Einbindung externer sowie interner Ressourcen gelten folgende Anforderungen:

- Es darf keine Ressource eingebunden werden, deren Identifikator durch ungefilterte Benutzereingaben definiert wird.
- Alle eingebundenen Ressourcen müssen definiert und in einer eigenen Liste bzw. einem eigenen Verzeichnis abgelegt werden.
- Der Zugriff ist auf Ressourcen zu beschränken, die für die Funktion der Webapplikation notwendig sind.
- Externe Ressourcen dürfen nur mit den minimal notwendigen Rechten verwendet werden.
- Die einzubindenden Ressourcen müssen so abgelegt werden, dass sie nicht unbefugt gelesen oder verändert werden können.

8 Behandlung von Datenausgaben

Die Webapplikation muss Filter, Kodierungen oder andere Methoden implementieren, die verhindern, dass Anwender oder andere Anwendungen über Datenausgaben der Webapplikation angegriffen werden können. Dabei müssen alle Kodierungsmöglichkeiten berücksichtigt werden, die es ermöglichen, Angriffsvektoren an die Anwender oder andere Anwendungen über die Webapplikation weiterzureichen.

9 Hintergrundsysteme

Unabhängig von der verwendeten Technologie muss die Webapplikation so implementiert werden, dass sie mit minimal notwendigen Rechten auf die benötigten Hintergrundsysteme zugreifen kann.

10 System- und Fehlermeldungen

System- und Fehlermeldungen sowie Kommentare dürfen keine Informationen an die Benutzer ausgeben, die in weiterer Folge für Angriffe auf das System genutzt werden könnten.

11 Kryptographie

Bei Einsatz von Kryptographie müssen standardisierte und an der jeweiligen Plattform erfolgreich getestete Algorithmen und Verfahren verwendet werden. Diese dürfen keine im Kontext der Anwendung des Verfahrens relevanten Schwachstellen aufweisen. Die verwendeten Schlüssel müssen eine ausreichend hohe Entropie und Zufälligkeit aufweisen.

Literaturhinweise

IT-Grundschutzhandbuch, *Standard-Sicherheitsmaßnahmen für den niedrigen bis mittleren Schutzbedarf*, Bundesamt für die Sicherheit in der Informationstechnik, Bundesanzeiger-Verlag, 2005

HTTP, *Hypertext Transfer Protocol*; <http://www.w3.org>

OWASP-Guide, *Open Web Application Security Project*; <http://www.owasp.org>

RFC 2616, *Hypertext Transfer Protocol – HTTP/1.1*; <http://www.rfc.net>

Wichtige Informationen für Norm-Anwender



Österreichisches
Normungsinstitut

Austrian Standards
Institute

Member of CEN and ISO

Normen sind Regeln, die im Dialog und Konsens aller Betroffenen und Interessierten entwickelt werden. Sie legen Anforderungen an Produkte, Dienstleistungen, Systeme und Qualifikationen fest und definieren, wie die Einhaltung dieser Anforderungen überprüft wird.

Von Ihrem Wesen her sind Normen Empfehlungen. Ihre Anwendung ist somit freiwillig, aber naheliegend, da Normen den aktuellen Stand der Technik dokumentieren: das, was in einem bestimmten Fachgebiet „Standard“ ist. Dafür bürgen das hohe Fachwissen und die Erfahrung der Experten und Expertinnen in den zuständigen Komitees auf nationaler, europäischer und internationaler Ebene – sowie die Kompetenz des Österreichischen Normungsinstituts und seiner Komitee-Manager.

Aktualität des Normenwerks. Analog zur technischen und wirtschaftlichen Weiterentwicklung unterliegen Normen einem kontinuierlichen Wandel. Sie werden vom zuständigen ON-Komitee laufend auf Aktualität überprüft und bei Bedarf überarbeitet und dem aktuellen Stand der Technik angepasst. Für den Anwender von Normen ist es daher wichtig, immer Zugriff auf die neuesten Ausgaben der Normen seines Fachgebiets zu haben, um sicherzustellen, dass seine Produkte und Produktionsverfahren bzw. Dienstleistungen den Markterfordernissen entsprechen.

Wissen um Veränderungen. Um zuverlässig über Änderungen in den Normenwerken informiert zu sein und um stets Zugriff auf die jeweils gültigen Fassungen zu haben, bietet „Austrian Standards plus Publishing“ den Norm-Anwendern zahlreiche und auf ihre Bedürfnisse zugeschnittene Angebote. Das reicht von klassischen Fachgebiets-Abonnements bis hin zu innovativen kundenspezifischen Online-Lösungen und Update-Services.

Normen & Regelwerke aus dem Ausland. Über »AS+P« können auch Internationale Normen (ISO) sowie Normen und Regelwerke aus allen Ländern der Welt bezogen werden – ein besonders wichtiger Service für die exportorientierte Wirtschaft. Ebenso sind Dokumente anderer österreichischer Regelschreiber bei »AS+P« erhältlich.

Austrian Standards plus Publishing (AS+P)


Heinestraße 38, 1020 Wien

E-Mail: sales@as-plus.at

www.as-plus.at/shop

Fax: +43 1 213 00-818

Tel.: +43 1 213 00-805

Austrian Standards plus 
Publishing

Weiterbildung zu Normen. Ein Plus an Wissen rund um Normen und ihr Umfeld bietet die »Austrian Standards plus Trainings«. In Seminaren, Vorträgen, Workshops und Lehrgängen bieten Experten, die zum Großteil selbst an der Entwicklung der Normen mitwirken, Informationen und Know-how aus erster Hand.

Austrian Standards plus Trainings (AS+T)


Heinestraße 38, 1020 Wien

E-Mail: trainings@as-plus.at

www.as-plus.at/trainings

Fax: +43 1 213 00-350

Tel.: +43 1 213 00-318

Austrian Standards plus 
Trainings

Normkonformität. Um die Einhaltung von Normen objektiv nachweisen zu können, bieten das Österreichische Normungsinstitut und »Austrian Standards plus Certification« die Möglichkeit der Zertifizierung von Produkten, Dienstleistungen und Personen auf Normkonformität.

Austrian Standards plus Certification (AS+C)


Heinestraße 38, 1020 Wien

E-Mail: certification@as-plus.at

www.as-plus.at/certification

Fax: +43 1 213 00-520

Tel.: +43 1 213 00-524

Austrian Standards plus 
Certification

Austrian Standards plus 
More Than Just Standards.

Die »Austrian Standards plus GmbH« ist ein
Unternehmen des Österreichischen Normungsinstituts