

## Web: Wie man Datenklau verhindert

**Unberechtigter Zugriff auf sensible Nutzerdaten im Internet kann unangenehme Folgen haben. Die neue ÖNORM A 7700 sagt, worauf es ankommt, um Hacker-Angriffe erfolgreich abzuwehren.**



Bildquelle: ON prm

Wien (ON/AS+ prm) Firmenspionage, Phishing, Computer-Hacks - der Datenklau mit zum Teil unabsehbaren Folgen wird immer professioneller. Wenn Sie selbst eine Webseite mit Applikationen anbieten, haben Sie alle Schwachstellen analysiert und abgesichert?

Unterstützung bietet die neue ÖNORM A 7700 "Informationsverarbeitung – Sicherheitstechnische Anforderungen an Webapplikationen", die mit 1. Dezember 2008 erschienen ist. Diese Norm ist eine Neubearbeitung der bislang gültigen ON-Regel ONR 17700 aus 2006 und unterscheidet sich grundlegend.

### Chancen & Risiken

Eine Webanwendung oder Webapplikation ist ein Computerprogramm, das auf einem Webserver ausgeführt wird, wobei die Interaktion mit dem Benutzer ausschließlich über einen Webbrowser erfolgt. Durch das Ausfüllen und Absenden eines Formulars übermittelt der Benutzer beispielsweise bei der Bestellung in einem Webshop Daten, die für die Abwicklung des Auftrags serverseitig in Datenbanken oder in Dateien gespeichert werden. Benutzerbezogene Daten können auch clientseitig durch HTTP-Cookies gespeichert werden.

Mit Webapplikationen kann man heutzutage über eine Internetanwendung vieles erledigen: eine Rechnung per Telebanking bezahlen, Waren über eine Auktionsplattform ersteigern, einen Flug buchen, Bilder auf eine Fotoplattform hochladen, einen Kommentar in einem Weblog verfassen ...

Unzählige Anbieter offerieren mittlerweile Online-Interaktionsmöglichkeiten mit Firmen, Menschen und weltweiten Communities. Viele dieser Anwendungen sind praktisch und sparen eine Menge Zeit, viele machen einfach nur Vergnügen. Aber wer weiß schon mit Sicherheit, was mit den Daten geschieht, die da-

### Hinweis

Erhältlich sind  
**ÖNORM A 7700** Informationsverarbeitung - Sicherheitstechnische Anforderungen an Webapplikationen  
**ÖNORM ISO/IEC 27001** Informationstechnologie - Sicherheitstechnik - Informationssicherheits-Managementsysteme - Anforderungen  
**ÖNORM ISO/IEC 27002** ... - Leitfaden für das Management der Informationssicherheit  
**ISO/IEC 20000** Information technology - Service management;  
Part 1: Specification; Part 2: Code of practice

im Webshop  
<http://www.as-plus.at/shop>

### ON Certified Website

Informationen zur Zertifizierung nach ÖNORM A 7700 bei:  
"Austrian Standards plus Certification"  
<http://www.as-plus.at/de/certification.html>

### Medienkontakt

Dr. Johannes Stern  
PR & Medien  
ON Österreichisches Normungsinstitut  
1020 Wien, Heinestraße 38  
Tel. +43 1 213 00-317  
Fax +43 1 213 00-327  
E-Mail: [johannes.stern@on-norm.at](mailto:johannes.stern@on-norm.at)  
Internet: <http://www.on-norm.at>

PR-ID: 0157-2008-12-01/ web\_datenklaue

bei ausgetauscht werden.

### **Zielscheibe für Hacker**

In den letzten Jahren werden Webanwendungen aller Art nachweislich immer stärker zur Zielscheibe von Hackerangriffen. Ob SQL Injection, Cross Site Scripting, Session Hijacking oder andere Methoden – die heimlichen Invasoren nutzen Schwachstellen ganz gezielt. Da die Netzwerkebene oft gar nicht berührt wird, können sie von klassischen IT-Sicherheitssystemen, wie Firewall oder IDS/IPS-Systemen, nicht erkannt und abgewehrt werden.

### **Trügerische Sicherheit**

Was gibt es Unangenehmeres, als das Opfer eines elektronischen Angriffs zu sein? Es gar nicht mitzubekommen! Während sich der Betreiber einer Webanwendung in trügerischer Sicherheit wiegt, werden seine wichtigen Kundendaten, Bezugswege oder Produktgeheimnisse ausgeschnüffelt, im schlimmeren Fall verändert oder gestohlen.

Mögliche schwerwiegende Auswirkungen eines solchen Einbruchs bzw. Diebstahls können die Unterbrechung betrieblicher Prozesse (auch bei Kunden oder Partnern) sein, von Imageverlust oder Schadenersatzforderungen ganz zu schweigen. Deshalb sollten auch vermeintlich "unwichtige" Webanwendungen zumindest gegen bekannte Angriffe gesichert werden.

Historisch betrachtet, wurde das Web, speziell das Protokoll HTTP, nicht für die heute üblichen komplexen Anwendungen konzipiert. Webapplikationen sind das schwächste Glied an der Schnittstelle zwischen Firmeninterna und Außenwelt, denn nur eine einzige Lücke kann unerwünschten Besuchern Zutritt gewähren.

### **Orten von Schwachstellen**

Damit es gar nicht so weit kommt, haben jetzt IT-Sicherheitsbeauftragte mit der ÖNORM A 7700 einen Leitfaden zur Hand, der in Form einer Checkliste hilft, firmeneigene Webapplikationen auf mögliche Schwachstellen penibel zu untersuchen.

Behandelt werden auch folgende Themen: Begriffe, Architektur der Webapplikation, Datenspeicherung und Datentransport, Konfigurationsdaten, Authentifizierung, Autorisierung und Sitzungen, Behandlung von Benutzereingaben bzw. Datenausgaben, Hintergrundsysteme, System- und Fehlermeldungen sowie Kryptographie.

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

#### **Sicherheit bestätigt**

So wie schon auf Basis der ONR 17700 können Webapplikationen, die die Anforderungen der ÖNORM A 7700 erfüllen, nach dem System "ON Certified Website" zertifiziert werden.