

## HELPDESK

# Web-Apps: Die Stolper- fallen

Jede Woche beantworten Sicherheits-  
experten Leserfragen und geben  
Ratschläge, wie sich die Sicherheit in  
einem Unternehmen erhöhen lässt.

## Frage: Wie kann ich die Sicherheit meiner Web-Applikation erhöhen?

Wer eine Web-Applikation entwickelt, spielt früher oder später mit dem Gedanken, diese auch per Internet zur Verfügung zu stellen. Es folgen die häufigsten Fehler, die bei Web-Applikationen gemacht werden.

### Authentisierung und Verschlüsselung

Die Authentisierung ist die Hürde, welche Unberechtigten den Zugriff auf die Applikation verweigert. Eine verschlüsselte Verbindung ist Pflicht und sollte erzwungen werden, indem Port 80 abgeschaltet oder auf Port 443 weiter geleitet wird. Die Verwendung «geheimer» Port-Nummern hat keinen Einfluss auf die Sicherheit. Die Authentisierung kann zweistufig oder dreistufig (z.B. mittels RSA-Token) realisiert werden. Eine dreistufige Authentisierung sollte so umgesetzt werden, dass der Benutzer sämtliche Angaben in der selben Maske eingeben muss. Die starke Authentisierung wird nämlich geschwächt, wenn erst nach dem erfolgreichen Anmelden mit Benutzername und Passwort nach dem Token gefragt wird. In keinem Fall

sollte die Applikation bei einem Fehlversuch angeben, ob der Benutzername oder das Passwort falsch war, da sich so gültige Benutzerkonten eruieren lassen.

Selbst gestrickte Verschlüsselungsalgorithmen sind zu vermeiden. Nicht umsonst gilt ein Algorithmus erst dann als sicher, wenn er einige Jahrzehn-

## «Fehlermeldungen dürfen keinen Aufschluss über die Systemarchitektur geben.»

te in der Wildnis überlebt hat. Eigenbau-Algorithmen sind eine Gefahr für die Applikation. Sie lassen sich durch die Verwendung von Libraries (z.B. OpenSSL oder Cryptography in .Net) mit wenigen Zeilen mit einem sicheren Algorithmus ersetzen.

### Dokumentation

Eine unzulänglich dokumentierte Software mag zwar funktionieren, ist jedoch nicht viel Wert. Wenn in einigen Jahren keiner der beteiligten Entwickler mehr in der Firma arbeitet, wird es sehr aufwändig, die Applikation zu warten. Meistens wird dies dann ganz unterlassen. Bemerkungen im Code sind zwar wichtig, aber nur für Programmierer.

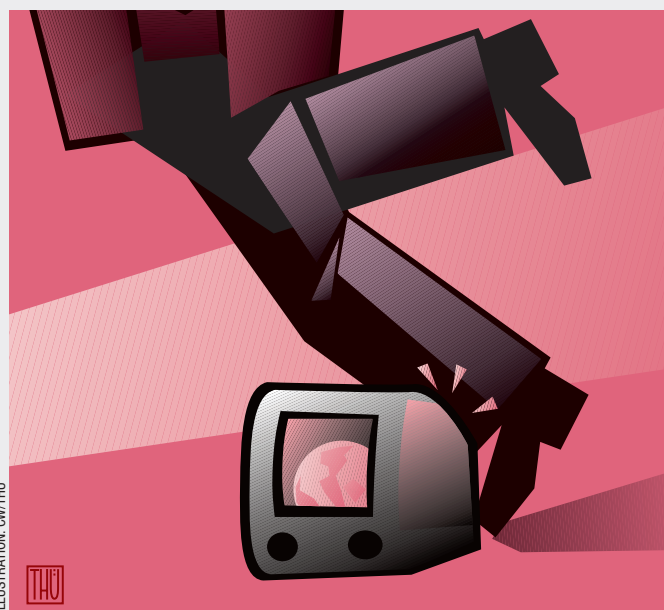


ILLUSTRATION: CW/THU

### Verschleierungen

Wer die Sicherheit der Applikation darauf aufbaut, dass einem Angreifer gewisse Informationen nicht zur Verfügung stehen, liegt falsch. So wie die erwähnten Portnummern können beispielsweise versteckte URLs keine Sicherheit bieten. Beim Design der Applikation sollte davon ausgegangen werden,

dass ein Angreifer die Applikation wie seine Westentasche kennt und ihm lediglich die Informationen zur Authentisierung fehlen. Diese geheim zu halten obliegt der Verantwortung der Benutzer.

### Patching und Hardening

Ist eine Applikation perfekt gesichert, setzt sie dennoch auf bestehenden Systemen auf. Diese sollten initial gehärtet und dann regelmässig gepatched werden. Bei IIS-Webservern werden beispielsweise gerne die http-Methoden «put» und «delete» vergessen, was Unberechtigten erlaubt, Dateien auf den Webserver zu laden oder zu löschen.

### Entwicklungszeit

Eine einfache Webapplikation ist schnell mal programmiert. Wem jedoch die Sicherheit ein Anliegen ist, sollte dafür auch genug Projektzeit einrechnen. Eine sichere Applikation ist

nicht nur vor Angriffen Unberechtigter geschützt, sondern auch vor legitimen Benutzern. Zum Beispiel sollte es nicht möglich sein, durch das Ändern der URL Berechtigungen eines anderen Benutzers zu erlangen. Unsichere Applikationen sind meist das Ergebnis von Zeitdruck.

### Eingaben und Fehlermeldungen

Die Applikation sollte sämtliche Benutzereingaben zuerst anhand eines Whitelist-Filters validieren. Der Blacklist-Ansatz ist weniger empfehlenswert, da der Programmierer nicht wissen kann, wie der Angreifer die Zeichen codiert. Auch die Länge sollte vor der Verarbeitung kontrolliert werden. Fehlermeldungen sollten so gestaltet sein, dass sie keinen Aufschluss über die Systemarchitektur ermöglichen. ■



**Der Autor**  
Simon Wepfer ist  
Consultant bei  
der Sicherheits-  
beraterin One-  
consult, Thalwil.  
www.onecon-  
sult.com

**Unsere Experten beantworten Ihre Fragen.** Schreiben Sie uns: [it-security@computerworld.ch](mailto:it-security@computerworld.ch)

**Ein Archiv der Helpdeskartikel finden Sie im Internet:**  
[www.computerworld.ch](http://www.computerworld.ch)