

heute.de computer

- ▶ heute-Nachrichten
- ▶ Startseite
- ▶ Schlagzeilen
- ▶ Politik
- ▶ Magazin
- ▶ Wirtschaft
- ▶ **Computer**
- ▶ Sport
- ▶ Wetter
- ▶ Börse

ZDFmediathek

Sendung verpasst?

▶ Jetzt ansehen



▶ ZDF heute

▶ ZDF heute journal

▶ ZDF heute nacht

Sendungen von A-Z ▶

- Service
- ▶ Podcast-Angebot
 - ▶ heute-Telegramm
 - ▶ Bildschirmschoner
 - ▶ PDA-Angebote
 - ▶ WAP-Dienste
 - ▶ Newsletter
 - ▶ RSS-Angebot
 - ▶ Nachrichtenbanner
 - ▶ Sidebar
 - ▶ heute als Startseite

Fehlerhafte Software: Die Liste des Schreckens

US-Institut veröffentlicht Liste der 25 gefährlichsten Programmierfehler

von Alfred Krüger und Volker Heil

Vom Phishing bis zum Datenklau - viele Übel, die den Surfer treffen können, werden erst durch Softwarefehler möglich. Die meisten Fehler sind vermeidbar, sagt ein US-Institut und hat eine Liste mit den 25 gefährlichsten Programmierfehlern erstellt.



Programmierfehler öffnen schädlicher Software, wie Trojanern, Tür und Tor. imago

Drucken Versenden 22.01.2009 [Archiv]

Die Eingangstür ist fest verschlossen. Ein Wächter steht davor. Einlass nur nach Passkontrolle. Einbrecher kommen aber selten durch den Haupteingang. Sie suchen nach der Hintertür. Und die ist vielfach schlecht gesichert. Manchmal steht sie sogar offen - aus Nachlässigkeit oder weil sie eben immer offen stand. Die ungebetenen Gäste dringen heimlich ein und holen sich das Tafelsilber.

Injektionen mit der Schädlingsspritze

Auch Cyberkriminelle nutzen ungesicherte "Hintertüren", um heimlich in die Rechner ihrer Opfer einzudringen. Solche Hintertüren finden sie in der benutzten Software und natürlich im Betriebssystem. Schuld sind Programmierfehler. Sie werden weidlich ausgenutzt. Daten-Phisher nutzen sie zum Passwortklau, Botnetzbetreiber zur Verbreitung von Trojanern und cyberkriminelle Hacker zum Einbruch in Rechenzentren. Das US-amerikanische SANS-Institut hat nun eine Liste mit den 25 häufigsten und gefährlichsten Programmierfehlern der letzten Jahre veröffentlicht - ein Register gängiger Programmiersünden.

Die Liste

▶ **Die 25 gefährlichsten Programmierfehler**

Das ZDF ist für den Inhalt externer Internetseiten nicht verantwortlich.

12. Dezember 2008: Sicherheitsspezialisten entdecken eine ungesicherte Hintertür in Microsofts Internet Explorer. Der Besuch entsprechend manipulierter Webseiten reicht aus, um schädliche Programme in den PC zu lassen. Selbst harmlose Webseiten können solche Schadprogramme beherbergen. Wie aber gelangen die Schädlinge auf diese Seiten? Für kriminelle Hacker ist das kein Problem. Sie greifen die Webserver an, auf denen die Webseiten gespeichert sind, und pflastern sie mit Schadprogrammen zu - oft per sogenannter SQL-Injection.

Programmierfehler machen solche Angriffe erst möglich. Ihr Ausmaß ist erschreckend. Die Zahl der Webseiten, die mit Hilfe einer solchen SQL-Giftspritze infiziert wurden, ist in den letzten Monaten explodiert. Jeden Tag kommen laut Sicherheitsunternehmen Sophos rund 15.000 neu infizierte Seiten hinzu. Ein großer Teil davon wurde mit Hilfe der SQL-Injection manipuliert - Grund genug für das SANS-Institut, den Programmierfehler, der eine solche Injektion mit schädlichem Programmcode zulässt, auf die Liste der gefährlichsten Programmiersünden zu setzen.

"Besser coden"

Dabei wäre es für einen versierten Programmierer im Grunde kein Problem, Angriffe wie den mit der Schädlingsspritze abzuwehren, meinen Experten. Ihr allgemeiner Ratschlag: "Besser coden" - also bessere Programme schreiben. Voraussetzung sei jedoch, dass sich die Programmierer der Tragweite möglicher Fehler überhaupt bewusst sind, sagt das SANS. Die Liste mit den weit verbreiteten Programmierfehlern soll deshalb das Problembewusstsein der einzelnen Programmierer, aber auch der Universitätsdozenten und der Softwareproduzenten schärfen.

"Wir sind immer wieder überrascht, welche wirklich grundlegenden Fehler die großen Unternehmen machen", sagt Thomas Kristensen vom Sicherheitsunternehmen Secunia. Das dänische Unternehmen war neben den Experten von SANS und Branchengrößen wie Microsoft, Symantec, Oracle und Linux-Firma Red Hat an der Erstellung der Fehlerliste beteiligt. Auch an den Universitäten werde noch immer nicht gelehrt, wie man sicherheitsrelevante Fehler erkennt und wie sie sich vermeiden lassen, monieren Experten.

"Die 25 Programmierfehler sind massiv verbreitet", erklärte SANS-Direktor Mason Brown. "Nun ist der richtige Zeitpunkt, sie zu schließen. Wir müssen sicherstellen, dass jeder Programmierer weiß, wie man ein Programm schreibt, das diese 25 Fehler nicht enthält" - Fehler etwa wie jene, die das unter Hackern sehr beliebte Cross-Site-Scripting möglich machen.

SANS-Liste wird 2009 fortgeführt

"Cross-Site-Scripting (XSS) ist eine der geläufigsten und gefährlichsten Schwachstellen in Webanwendungen", heißt es im SANS-Bericht. Besonders betroffen sind Web-2.0-Anwendungen. Beim Cross-Site-Scripting versuchen Cyberkriminelle, schädlichen Programmcode in eine legitime Webseite einzubetten. Wenn der Nutzer diese Seite aufruft, wird der Schadcode aktiviert. Die Angreifer können dem Surfer auf diesem Wege beliebige Seiteninhalte vorgaukeln, um ihm Passwörter oder Kontodaten zu entlocken. Fehlerhaft programmierte Anwendungen machen solche cyberkriminellen Machenschaften möglich.

Alle Programmierfehler, die auf der SANS-Liste aufgeführt werden, seien einfach zu entdecken und von böswilligen Hackern ebenso leicht auszunutzen, heißt es im Bericht des SANS. Die unzureichende Absicherung von Nutzereingaben in Webformularen wird hier ebenso gelistet wie etwa Mängel bei der Regelung von Benutzerrechten. Programmierfehler können darüber hinaus zu falschen Berechnungen mit unlogischen Ergebnissen führen, die ein Programm im ungünstigsten Fall abstürzen lassen und Datenverluste nach sich ziehen können.

Die SANS-Liste werde im nächsten Jahr fortgeführt, erklärte Bob Martin, Chef des gemeinnützigen US-Unternehmens MITRE, das das Projekt zusammen mit dem SANS-Institut auf die Beine gestellt hat. An Fehlernachschub dürfte es dabei nicht mangeln. Denn schon in diesem Jahr mussten sich die SANS-Experten durch einen Wust von über 700 Softwarefehlern kämpfen.

Drucken Versenden zum Seitenanfang ▶

Mehr zum Thema

- ▶ **Wie man Datenspione ausspioniert**
Forscherguppe der Uni Mannheim leimt cyberkriminelle Datendiebe
- ▶ **2009 gibt es deutlich mehr Cyberkriminalität**
Sicherheitsunternehmen mit düsteren Prognosen
- ▶ **Deutsche Rechner unter fremder Kontrolle**
Die meisten infizierten Rechner stehen in den USA und China
- ▶ **BKA: Deutschland ist Testweise für Online-Kriminelle**
Fortschrittlicher PC-Schutz gilt als "Herausforderung"
- ▶ **Webprofile: Leichtes Spiel für Datenklauer**
Wie Cyberkriminelle Personensuchmaschinen für ihre Zwecke nutzen
- ▶ **"Stasi" im Internet**
Netzwerk-User geben freiwillig massenweise intime Daten preis
- ▶ **Phishing: Nur "große Fische" im Visier**
Cyberkriminelle greifen gezielt wohlhabende US-Unternehmer an



Externe Links

- ▶ **Liste der 25 gefährlichsten Programmierfehler**
- Das ZDF ist für den Inhalt externer Webseiten nicht verantwortlich