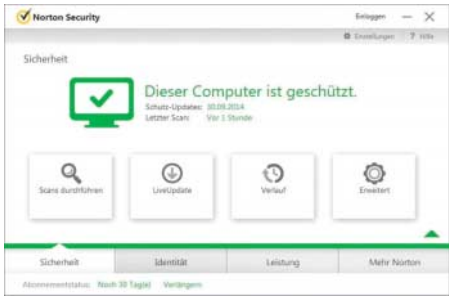
## Symantec gibt Norton AntiVirus auf

Symantec bietet seinen traditionsreichen Virenjäger Norton AntiVirus nicht länger an. Die diesjährige Norton-Generation verkauft das Unternehmen nur noch als Gesamtpaket „Norton Security“ mit Firewall, Identitätsschutz und Co. Wer Norton AntiVirus bereits besitzt, soll seine Lizenz weiterhin verlängern können und auch Signatur-Updates erhalten. Aktuell kann man im Handel noch Restbestände kaufen.




Die Größe der lokal gespeicherten Schädlingssignaturen will das Unternehmen durch eine engere Verzahnung mit der Norton Cloud um 80 Prozent verkleinert haben. Norton Security kostet als Einzellizenz 40 Euro pro Jahr. Für 60 Euro bekommt man fünf Lizenzen, die man je nach Bedarf auf Windows-Rechnern, Macs sowie Android- und iOS-Geräten einsetzen kann. (rei)

**Gegenüber der Vorjahreskollektion bietet Norton Security unter anderem eine abermals vereinfachte Oberfläche sowie eine neue Generation der Antimalware-Engine.**

## Shellshock zähmen

Für die in c’t 22/14 auf Seite 46 gemeldeten Shellshock-Sicherheitsprobleme gibt es inzwischen Patches, die alle bisher bekannt gewordenen Lücken schließen. Im einfachsten Fall genügt es, das System über den Paketmanager auf den aktuellen Stand zu bringen; Mac-Nutzer müssen das benötigte Sicherheits-Update manuell von der Apple-Seite herunterladen und installieren (siehe c’t-Link). (rei)

c't Apple-Update: ct.de/yus4

## Webinar gegen App-Wildwuchs

Apps für Smartphones und Tablets sind im Unternehmenseinsatz unter Umständen eine echte Gefahr. Aufgrund des hohen Verbreitungsgrades von iPhones und iPads sowie der Vertraulichkeit der auf diesen Geräten verarbeiteten Daten ergeben sich hohe Sicherheitsanforderungen an das iOS-Betriebssystem sowie dessen Apps. heise Security veranstaltet am 30. Oktober 2014 ein Webinar, das nicht nur auf die Gefahren aufmerksam macht, sondern auch erklärt, wie man Smartphones und Apps richtig testet, um eine saubere Policy zu erstellen und umzusetzen. Am Beispiel von iOS werden zahlreiche Sicherheits- und Datenschutzprobleme mobiler Apps demonstriert – die Prinzipien sind auch auf Android oder Windows Phone übertragbar. Anhand von Schwachstellen in weit verbreiteten Apps werden häufige Programmier- und Design-Fehler erläutert, die zu Sicherheitsproblemen führen.

Im Rahmen von Live-Demonstrationen erörtert der Referent Andreas Kurtz die wichtigsten Fragen und stellt Methoden sowie Werkzeuge vor, mit denen sich iOS-Apps auf Sicherheitsprobleme hin untersuchen lassen. Die Teilnahme kostet 90 Euro.

(Matthias Parbel/rei)

c't Webinar: ct.de/yus4



## Bösartige USB-Sticks selbst gemacht

Mit öffentlich zugänglichen Tools kann man einen herkömmlichen USB-Speicherstick in einen gefährlichen BadUSB-Angriffstick verwandeln. Der Sicherheitsforscher Kasten Nohl hatte Ende Juli für Aufsehen gesorgt, als er auf die zuvor wenig beachtete Gefahr durch speziell präparierte USB-Geräte aufmerksam machte. So kann ein Stick mit einer manipulierten Firmware blitzschnell Tastatureingaben an den Rechner des Opfers schicken und so etwa eine Backdoor installieren. Dazu meldet sich der Speicherstick als USB-Tastatur an, die das System automatisch erkennt und einbindet. Die zur Modifikation des Sticks genutzten Tools hielt Nohl unter Verschluss. Die Forscher Adam Caudill und Brandon Wilson konnten Nohls Arbeit allerdings nachvollziehen und haben alle nötigen Werkzeuge ins Netz gestellt. Der kürzlich in c’t vorgestellte, kostenlose G Data USB Guard schützt vor diesem Angriff (siehe c’t-Link).

Neben der Tastatur-Simulation entwickelten die beiden Forscher weitere Angriffe: Man kann den Stick etwa so programmieren, dass er eine versteckte Partition enthält, die erst sichtbar wird, wenn man die sichtbare Partition vom Betriebssystem auswerfen lässt. Einen geeigneten Speicherstick wie den Patriot PSF8GXPUSB Supersonic Xpress bekommt man schon für unter zehn Euro. Die Tools unterstützen Sticks, die auf dem Controller Phison 2251-03 basieren. (rei)

c't USB Guard: ct.de/yus4