

„Schweigegeld-Deal im Netz“ titelt Heise Security!

Hacker haben den **kompletten Quellcode** der Symantec Security Produkte entwendet und inzwischen bereits teilweise im Internet veröffentlicht.

pcAnywhere und **Norton Utilities** sind bereits verfügbar, **Norton Antivirus** und **Norton Internet Security** dürften in Kürze folgen. Im Raum steht die Behauptung, dass Symantec dem Hacker 50.000 US-Dollar geboten hat, damit dieser die Quellen nicht weiter gibt. Hacker und Symantec behaupten, dass sie den jeweils anderen mit „Schweigegeldangebot/-forderung“ aus der Reserve locken wollten.

Sei es drum!

Der Quellcode liegt jetzt offen, wie bei einem OPEN Source Projekt.

Jeder potentielle Angreifer kann sich nun leicht detailliert in die Arbeitsweise der Sicherheitsprodukte einlesen und gezielt Angriffe ausarbeiten. Die Sicherheitsprodukte drohen, komplett unterwandert zu werden. Das Auffinden von Lücken und Angriffspunkten - ohne Quellcode ein aufwendiges und kompliziertes Unterfangen - wird jetzt quasi zum Kinderspiel. Ein Chaos, bei dem Norton gegen sich selbst kämpfen wird.

Symantec warnt inzwischen zumindest vor dem Einsatz von pcAnywhere. Wahrscheinlich ist dies genau das Produkt, mit dem am wenigsten Umsatz gemacht wird?!

Setzen Sie die „Open - Source“ Produkte der NORTON Reihe von Symantec weiter ein? Oder haben Sie die in den USA unter Scareware-Anklage stehenden Produkte überhaupt noch eingesetzt?

[Anmerkung zu **Scareware**: - Es gehört aus meiner Sicht in die unterste Schublade, wenn man künstlich mit einem „Sicherheitsprodukt“ Panik schürt, um den Anwender in seiner vermeintlichen Not zum Kauf zu nötigen!]

Zum Artikel bei Heise:

[pcAnywhere-Code nach geplatztem Schweigegeld-Deal im Netz | heise Security.](#)