

Pseudonymisierung schützt

IT-Sicherheit muss auch den **Datenschutz** beachten. Dies zeigt der Workshop Privacy Respecting Incident Management (**Prima**) der Gesellschaft für Informatik (www.gi-fg-sidar/prima 2005). So betont die Rechtsanwältin Ursula Sury, dass beim Sammeln von Netzdaten etwa über Intrusion Detection Systeme, die nötige Transparenz zu gewährleisten sei. Mitarbeiter und Betriebsräte sind zu informieren, Daten dürfen nicht zu lange gespeichert werden.



Workshop-Mitinitiator Ulrich Flegel von der Uni Dortmund Dortmund verweist auf die Pseudonymisierung: „Überall wo personenbezogene Daten wie Benutzer-

name oder IP-Adresse geloggt werden, ist eine Pseudonymisierung möglich und angebracht.“ Durch den Einsatz von Kryptografie lassen sich Pseudonyme so erstellen, dass sie nur bei Auftreten von vorab festgelegten Verdachtsmomenten aufgedeckt werden können. Ergebnis dieser Forschungen an der Uni Dortmund ist das Open-Source Tool Pseudo/Core, das derzeit noch stärker auf den Einsatz im Bereich Intrusion Detection zugespißt wird, so Flegel. Ähnliches schlagen Stefan Köpsell und Kollegen an der Uni in Dresden für den beliebten Anonymisierungsdienst JAP vor. Auf richterliche Verfügung kann der Dienst die surfende und die angesurften IP-Adressen aufdecken. Flegel: „Im Sinne der Verhältnismäßigkeit eine sehr schöne Lösung, die generell die Anonymität sicherstellt und im Einzelfall die Strafverfolgung ermöglicht.“