Netzsicherheit und Datenschutz - alles PRIMA?

Ulrich Flegel, Marit Hansen, Michael Meier

PRIMA war der Titel eines Workshops, der im April 2005 in Regensburg im Rahmen der Konferenz „Sicherheit 2005“ stattfand, und steht für „Privacy Respecting Incident Management“. So richtig prima ist die Situation bei der Absicherung von lokalen Netzen (noch) nicht: Vielfach gibt es gar kein funktionierendes „Incident Management“, und wenn doch, dann spielen Datenschutzmaßnahmen für die Betreiber dieser Netze kaum eine Rolle.

Unter Incident Management versteht man den gesamten organisatorischen und technischen Prozess der Reaktion auf erkannte oder vermutete Sicherheitsvorfälle bzw. Störungen in IT-Bereichen sowie hierzu vorbereitende Maßnahmen und Prozesse. (Näheres ist dem Gateway dieses Hefts von *Wilhelm Dolle* zu entnehmen.) Hier ist nicht unbedingt das aktive Aufspüren und Verfolgen von Hackern oder Crackern vonnöten, die im eigenen System gewildert haben. Dies liefert zwar manch spannende Geschichte für Bücher[1] oder Filme, aber ist für die meisten Unternehmen viel zu aufwändig und mit eigenem Personal nur in seltenen Fällen leistbar.

Während bei Organisationen bisher vorrangig präventive Maßnahmen und Mechanismen im Vordergrund standen, wird zunehmend deutlich, dass IT-Sicherheit nicht allein durch Prävention erreichbar ist. Vielmehr stellt Prävention einen Grundpfeiler dar, neben dem ergänzend die reaktiven Aspekte der IT-Sicherheit stehen.

Mit diesen reaktiven Aspekten beschäftigt sich die Fachgruppe SIDAR (Security - Intrusion Detection and Response) des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI). Themen ihrer Arbeit sind Verwundbarkeitsanalyse von IT-Systemen, Intrusion Detection und Malware-Bekämpfung sowie Incident Management und IT-Forensik. Beim Entwurf und Einsatz der hierfür verwendeten Technologien werden Gesichtspunkte des Datenschutzes gegenwärtig nur selten berücksichtigt.

Dies wirft unmittelbar die Frage auf, ob eine datenschutzfördernde Technikgestaltung mit den Zielen reaktiver Sicherheit vereinbar ist. Um dieser Frage nachzugehen, veranstalteten die Fachgruppen SIDAR und PET (Privacy Enhancing Technologies) den PRIMA-Workshop, dessen Beiträge in diesem Heft zusammengefasst sind.

Zu diesem Heft

Zum Auftakt erläutert *Alexander Dix* (vormalig: Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg; nun Berliner Beauftragter für Datenschutz und Informationsfreiheit) die Datenschutzsicht von Incident Management. Beginnend beim klassischen Spannungfeld der oftmals unterschiedlichen Interessen von Security und Privacy stellt er Anforderungen an eine Protokollierung und Dokumentation dar und kommentiert dann den aktuellen Trend zur Vorratsdatenspeicherung.

Weitere rechtliche Aspekte werden in den beiden folgenden Artikeln beleuchtet: Während die Schweizer Rechtsanwältin und Professorin für Informatikrecht *Ursula Sury* in ihrem Beitrag „Datenschutzgerechte Nutzung von Intrusion Detection - Organisatorische und juristische Implikationen“ juristische und praktische Anforderungen an Intrusion Detection-Systeme und ihren datenschutzgerechten Betrieb formuliert, geht der Oberstaatsanwalt *Jens Gruhl* in „Private investigation“ im Bereich der IuK-Kriminalität“ auf die Zulässigkeit und Verwertbarkeit der Sachverhaltsaufklärung durch Geschädigte oder Dritte ein.

Anschließend wird die Betrachtung um Aspekte zur datenschutzfördernden Technikgestaltung erweitert. Vorgestellt wird der Beitrag „Strafverfolgung trotz Anonymität - Rechtliche Rahmenbedingungen und technische Umsetzung“ von *Stefan Köpsell* und *Tobias Miosga* von der TU Dresden, in dem die Autoren für den auf Mixkaskaden beruhenden Anonymisierungsdienst und vom BMWA geförderten Projekt „AN.ON – Anonymität online“ Konzepte und Randbedingungen für Strafverfolgung darlegen.

Ein anderes staatlich gefördertes Projekt zu Anonymität steht im Fokus des letzten Artikels „Mit Affen-Spielzeug etwas über Haustiere lernen“. *Ulrich Flegel* zeigt am Beispiel eines Audit-Daten-Pseudonymisierers die Verwendung von Bausteinen, die im APES-Projekt der KU Leuven beschrieben werden (APES: Anonymity and Privacy in Electronic Services).

Intrusion Detection ist das Thema des DuD-Forums: *Dirk Fox* unterzieht Intrusion Dectection-Systeme einem Reality-Check und hält sie für gescheitert; *Benjamin Fabian* dagegen verteidigt sie am Beispiel des Fallenstellens durch „Honeypots“.

Weitere Arbeit an dem Thema

Die Fachgruppen SIDAR und PET werden das Thema „Privacy Respecting Incident Management“ weiter verfolgen und laden zur Mitarbeit ein. Interessierte können sich auf der Website informieren:
http://www.gi-fg-sidar.de/

[1] Z.B. Die autobiographischen Bücher von Clifford Stoll: „Kuckucksei, Die Jagd auf die deutschen Hacker, die das Pentagon knackten“ (1989) und Tsutomu Shimomura: „Takedown“ (1996).