

CERT News

Datenschutz auch bei CERTs

Am 6. April 2005 fand in Regensburg der GI-Workshop „Privacy Respecting Incident Management“ (PRIMA 2005) statt
– eine Zusammenfassung

Sicherheit und Datenschutz sind zwar verwandt, haben aber häufig – zumindest vordergründig – gegenläufige Ziele. Während beispielsweise das eine möglichst viele Informationen zur Analyse von Schwachstellen und Angriffen sammeln möchte, steht beim anderen die Datensparsamkeit hoch im Kurs. Ein Workshop der deutschen Gesellschaft für Informatik e. V. (GI) hat sich unlängst dieses Spannungsfelds angenommen.

Die Fachgruppe SIDAR (Security – Intrusion Detection and Response) des GI-Fachbereichs Sicherheit fokussiert die reaktiven Aspekte der IT-Sicherheit sowie ihr Umfeld. Im Besonderen befasst sich die Fachgruppe mit der Verwundbarkeitsanalyse von IT-Systemen, mit Intrusion Detection und Malware-Bekämpfung sowie Incident-Management und IT-Forensik. Beim Entwurf und Einsatz der hierfür verwendeten Techniken werden Gesichtspunkte des Datenschutzes zwar als wichtig erkannt, aber tatsächlich zeigen sich oft entgegengesetzte Ziele.

Die Fachgruppe PET (Privacy Enhancing Technologies) betrachtet hingegen – ebenfalls im GI-Fachbereich Sicherheit – datenschutzfördernde Technik, allem voran Datenvermeidung und Datensparsamkeit, System- und Selbstdatenschutz, Transparenz und vertrauensbildende Maßnahmen – alles unter einem interdisziplinären Ansatz.

So lag es nahe, als Teil der Jahrestagung 2005 des Fachbereichs einen gemeinsamen Workshop zu veranstalten. Alle Präsentationen und Beiträge sind auf der PRIMA-Web-Seite www.gi-fg-sidar.de/prima2005/ verfügbar.

Zum Auftakt der Veranstaltung sprach Dr. Alexander Dix, der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg, über die Datenschutzsicht des Incident Management. Weitere rechtliche Aspekte wurden in den Vorträgen „Organisatorische und juristische Implikationen bei der datenschutzgerechten Nutzung bzw. Durchführung des Einsatzes von Intrusion Detection“ und „Private Investigation im Bereich der IuK-Kriminalität“ beleuchtet. Anschließend wurde die Betrachtung um Aspekte zur datenschutzfördernden Technikgestaltung erweitert. Vorgestellt wurden die Beiträge „Strafverfolgung trotz Anonymität – Rechtliche Rahmenbedingungen und technische Umsetzung“ und „Evaluating the Design of an Audit Data Pseudonymizer Using Basic Building Blocks for Anonymity“.

Eine Podiumsdiskussion zum Thema „Privacy Respecting Incident Management – Status und künftige Entwicklungen“ brachte zudem die verschiedenen Positionen von Vertretern der Datenschutzbeauftragten, der Ermittlungsbehörden sowie aus Forschung und Wirtschaft aufs Tapet. Zwischen dem Podium und den etwa 60 Teilnehmern entwickelte sich eine lebhaft diskutierte Diskussion, insbesondere über die Verhältnismäßigkeit der von Strafverfolgungsbehörden geforderten Vorratsdatenspeicherung.

Kritische Stimmen stellten zudem den Wert von Intrusion-Detection-Systemen (IDS) infrage: Nachdem vor einigen Jahren begonnen wurde, IDS als notwendige Komponente für die IT-Sicherheit anzusehen, ist in der jetzigen, wirtschaftlich für viele Unternehmen schwierigeren Lage das Interesse nicht mehr so groß.

Auch die Verwertbarkeit der gesammelten „Beweise“, beispielsweise vor Gericht, ist oft nicht gegeben, da menschliche Zeugen bevorzugt werden.

Ähnlich kontrovers wurde der massenhafte Anstieg bei Phishing-E-Mails diskutiert. Im Gegensatz zu anderen Ländern gibt es in Deutschland kaum nennenswerte Schäden, sodass manche das Problem bereits als „erledigt“ ansehen. Die Diskussion über Phishing führte jedoch auch zu der grundsätzlichen Frage, wo denn im Internet Sicherheitsmechanismen überhaupt ansetzen sollten – Ergebnis: Teledienstanbieter sollten selbst ausreichende Sicherheitsmaßnahmen ergreifen, anstatt Missbrauchsfälle in Kauf zu nehmen und dann auf eine nachträgliche Ermittlung durch Strafverfolgungsbehörden anhand von IP-Adressen mit fragwürdigem Beweiswert zu drängen. Aber die Realität sieht leider anders aus, wobei gerade die wieder diejenigen Nutzer ins Feld geführt wurden, die für mehr Sicherheit nicht mehr zahlen möchten. ■

Dieser Artikel basiert auf dem Protokoll des Workshops von Ulrich Flegel (Uni Dortmund), Marit Hansen (ULD Schleswig-Holstein) sowie Michael Meier (TU Cottbus).

Die Rubrik *CERT News* berichtet über aktuelle Entwicklungen aus dem Umfeld von Computer Emergency bzw. Security Incident Response Teams (CERTs/CSIRTs). Betreuer dieser Kolumne ist **Klaus-Peter Kossakowski** (www.kossakowski.de), der bereits ab 1992 mit dem Aufbau des ersten CERTs in Deutschland betraut war und seit Juni 2003 Vorsitzender des internationalen Dachverbands FIRST (www.first.org) ist.