Effektives kooperatives Sicherheits-Monitoring

Michael Meier

Cyberkriminelle und weitere Angreifer sind heute in der Lage mit nur geringem zeitlichem und finanziellem Aufwand weltweit Opfer zu selektieren und anzugreifen. Das Internet eröffnet Möglichkeiten simultan Angriffe in verschiedenen geographischen Regionen durchzuführen. Angriffswerkzeuge werden kontinuierlich optimiert um Sicherheitsmechanismen wie Intrusion-Detection-Systeme, Antiviren-Scanner oder Firewalls zu umgehen. Die rechtzeitige Reaktion auf diese sich verändernden Bedrohungen stellt IT-Sicherheits-Ingenieure und IT-Sicherheits-Analysten vor große Herausforderungen, die effektive Methoden für ein kooperatives Sicherheits-Monitoring zur Unterstützung des Austauschs von Monitoring-Daten, der kollaborativen Analyse von Beobachtungen sowie der Entwicklung von Erkennungs- und Mitigations-Ansätzen erfordern. In diesem Themenfeld arbeitet die AG IT-Sicherheit. Der Vortrag thematisiert ausgewählte aktuelle Forschungsarbeiten in diesem Themengebiet.