Forschungsschwerpunkte – Prof. Dr. Sascha Fahl

Sascha Fahl geht der Fragestellung nach, welchen Einfluss der Faktor Mensch auf IT-Sicherheits- und Datenschutzmechanismen hat. Während eine Vielzahl dieser Mechanismen theoretisch ein sehr hohes Maß an Schutz bietet, sieht die Praxis häufig ganz anders aus. Es zeigt sich immer wieder, dass das Maß von IT-Sicherheit und Datenschutz nicht nur von technischen Innovationen abhängt. Vielmehr ist es so, dass technische Lösungen so gestaltet sein müssen, dass sie von ihren jeweiligen Nutzerinnen und Nutzern möglichst einfach und sicher genutzt werden können. Um das Themenfeld der benutzbaren IT-Sicherheit zu erforschen, kombiniert Herr Fahl bekannte Methoden aus der IT-Sicherheit mit qualitativen und quantitativen Forschungsmethoden aus den Sozialwissenschaften und der Psychologie.

Während sich der Forschungsbereich der benutzbaren IT-Sicherheit klassischerweise mit Endnutzern beschäftigt und Fragen wie etwa der sicheren und einfach benutzbaren Mechanismen zur Authentifizierung oder der Verbesserung der Effektivität von Warnungsmeldungen nachgeht, verfolgt Herr Fahl in seinen Forschungsarbeiten einen ganzheitlichen Ansatz. Er erforscht nicht nur Endnutzer als eine wichtige Nutzergruppe von IT-Sicherheits- und Datenschutzmechanismen, sondern erstreckt seine Arbeiten auf alle zentralen Akteure wie etwa Softwareentwickler, Systemadministratoren oder Designer von IT-Systemen. Vergangene und aktuelle Forschungsprojekte, an denen seine Gruppe arbeitet, beschäftigen sich etwa mit Fragen, wie Werkzeuge für Softwareentwickler, kryptografische APIs oder Entwicklerdokumentation gestaltet werden müssen, damit Entwicklerinnen und Entwickler einen möglichst einfachen Zugang zu sicherer Softwareentwicklung bekommen können.

Eine aktuelle Forschungsarbeit in seiner Gruppe untersucht die Fragestellung, welchen Einfluss Informationsquellen, welche Softwareentwickler während der Bearbeitung von sicherheitsrelevanten Programmieraufgaben benutzen, auf die Sicherheit von Software haben. In einem kontrollierten Laborexperiment mit Entwicklerinnen und Entwicklern von Android-Applikationen konnte das Forschungsteam nachweisen, dass Informationsquellen wie etwa API-Dokumentationen von Herstellern in vielen Fällen zu schlecht und umständlich bedienbar sind. Entwickler greifen in diesen Fällen auf einfacher zugreifbare Informationen auf Frage- und Antwortplattformen, wie etwa Stack Overflow, zurück. In vielen Fällen sind solche Lösungen allerdings unsicher und tragen maßgeblich zu Schwachstellen in der Software bei. In einer anschließenden Untersuchung von mehr als 1,5 Millionen mobilen Android-

Applikationen konnte das Team um Sascha Fahl dieses Phänomen auch außerhalb des Labors nachweisen und bestätigen, dass eine Vielzahl von Schwachstellen in Android-Applikationen durch das Kopieren von unsicheren Codebeispielen von Stack Overflow verursacht werden. Diese Arbeiten wurden im letzten Jahr Gewinner der jährlichen „Best Scientific Cybersecurity Paper Competition“ der NSA. Um Entwicklerinnen und Entwickler in Zukunft besser bei der Lösung von sicherheitsrelevanten Fragestellungen bei der Softwareentwicklung zu unterstützen, arbeiten Herr Fahl und seine Gruppe gerade an neuartigen Konzepten zur Gestaltung und Umsetzung von sicherheitskritischer Entwicklerdokumentation, wobei das Team durch einen Google Faculty Research Award unterstützt wird.

Eine zweite Forschungsarbeit, an der Herr Fahl gemeinsam mit dem Sicherheitsteam des Google-Chrome-Browsers gearbeitet hat, geht der Fragestellung nach, wodurch HTTPS-Zertifikatswarnungsmeldungen in Webbrowsern verursacht werden. Während sich vergangene Arbeiten vor allem damit beschäftigten, wie Warnmeldungen für Endnutzer derart gestaltet werden können, damit weniger der Meldungen durch Nutzerinnen und Nutzer übergangen werden, haben diese Arbeiten ignoriert, dass viele Zertifikatswarnungen fälschlicherweise angezeigt werden. Endnutzer werden in vielen Fällen mit Warnmeldungen konfrontiert, obwohl gar kein Sicherheitsproblem vorliegt. In einer sechsmonatigen Felduntersuchung von Chrome-Nutzern konnte Fahl zusammen mit dem Sicherheitsteam des Google-Webbrowsers mehrere 100 Millionen Zertifikatswarnungen analysieren. Das Forscherteam konnte unterschiedliche Ursachen identifizieren. So tragen beispielsweise fehlerhaft konfigurierte Uhren auf Computern von Endnutzern oder Antivirensoftware zu einer Vielzahl falscher Warnmeldungen bei. Als Ergebnis dieser Forschungsarbeit wurden neuartige Meldungstypen entwickelt, die Endnutzern dabei helfen, Fehlkonfigurationen zu beheben und die zukünftige Zahl falscher Zertifikatswarnungen zu reduzieren. Diese Meldungen sind mittlerweile Bestandteil aller aktuellen Google-Chrome-Installationen und tragen zur Sicherheit von mehreren hundert Millionen Internetnutzern bei.

Diesen ganzheitlichen Ansatz wird Herr Fahl in Zukunft verfolgen und damit weitere zentrale Herausforderungen der IT-Sicherheit und des Datenschutzes erforschen.