Darüber hinaus werden der aktuelle Rechtsetzungsrahmen wie das SEPA-Begleitgesetz, das E-Government-Gesetz und der Entwurf der einschlägigen EU-Verordnung erörtert, die ab 2015 das deutsche Signaturgesetz teilweise obsolet werden lassen könnten.

Programm und Anmeldung unter: *http://www.teletrust.de/veranstaltungen/signaturtag/infotag-elektronische-signatur-2013/*

Forschungsprojekt „eID Connect" verifiziert das Alter mit Hilfe der CodeMeter-Technologie

Das Forschungsprojekt „eID Connect" wird vom Bundesministerium für Wirtschaft und Technologie unter dem Förderkennzeichen 2076918ED geführt; es verwaltet unterschiedliche elektronische Identitäten für beliebige Webdienste über OpenID, kombiniert mit Sicherheit und Benutzerfreundlichkeit. Dieses „Identity-as-a-Service" nutzt zur Authentifizierung den neuen elektronischen Personalausweis (nPA) oder die Schutzhardware CmDongle als Sicherheitstoken: beides erweitert die klassische Identifizierung mit Benutzername und Passwort.

Am Ende der 16-monatigen Projektzeit zeigen das FZI Forschungszentrum Informatik und die Karlsruher Unternehmen CAS Software AG, fun communication GmbH und Wibu-Systems AG einen ersten Prototypen. Das Ergebnis ist eine komplette Infrastruktur auf Basis von OpenIDs für virtuelle Identitäten, was beispielsweise bei manipulationssicherer Altersverifikation für Webseiten oder Video-on-Demand hilfreich ist. Das neue Verfahren kommt als SaaS-Lösung beim Provider und im mobilen Umfeld zum Einsatz und wird auf *www.eid-connect.de* beschrieben. Ein Test des Prototypen ist auf Nachfrage möglich.

Über einen OpenID-Server können Benutzer ihre virtuelle Identität selbst anlegen. Die virtuelle Identität kann mit Daten des neuen Personalausweises und eines CmDongles ergänzt werden. Der Benutzer bekommt so einen virtuellen Ausweis, den er nur in Kombination mit dem echten elektronischen Personalausweis, dem passenden CmDongle oder der Kombination aus Benutzername/Passwort verwenden kann. Auf diese Weise werden Daten wie Name, Alter, Adresse oder das Überschreiten einer bestimmten Altersgrenze verifiziert.

Strategiebericht Entwicklung sicherer Software

Hersteller von Software sehen in der IT-Sicherheit sowohl ein Risiko als auch eine Chance im globalen Wettbewerb. Die drei vom Bundesministerium für Bildung und Forschung (BMBF) geförderten deutschen Kompetenzzentren für IT-Sicherheit – CISPA, EC SPRIDE und KASTEL – unterstützen Hersteller bei der Entwicklung von sicherer Software: In ihrem aktuellen Trend- und Strategiebericht „Entwicklung Sicherer Software durch Security by Design" erörtern sie Herausforderungen und Lösungswege.

KASTEL ist als Kompetenzzentrum für Angewandte Sicherheits-Technologie am Karlsruher Institut für Technologie (KIT) angesiedelt.

Unter dem Dach des Fraunhofer Instituts SIT in Darmstadt arbeitet das Kompetenzzentrums European Center for Security and Privacy by Design (EC SPRIDE).

Das Center for IT-Security, Privacy Accountability (CISPA) arbeitet an der Universität Saarbrücken.

Softwarehersteller wissen: IT-Sicherheit ist neben der eigentlichen Funktionalität eine immer wichtigere Produkteigenschaft. Um Softwareprodukte sicherer zu machen, müssen IT-Sicherheitsfragen von Beginn des Herstellungsprozesses an berücksichtigt werden. Bezieht man sie zu spät ein, können neben den Kosten für die nachträgliche Behebung von Schwachstellen möglicherweise sogar Schadensersatzklagen sowie ein langfristiger Image- und Vertrauensverlust drohen. In Zukunft werden sich die Probleme noch verstärken: Die Komplexität von Software wird weiter zunehmen und die nachträgliche Absicherung von Software wird immer aufwendiger und teurer. Eine frühe systematische Berücksichtigung von Sicherheit bei der Softwareherstellung hat eine strategische Dimension und wird zum Wettbewerbsvorteil. Die Kompetenzzentren CISPA, EC SPRIDE und KASTEL zeigen der Softwareindustrie in ihrem Trend- und Strategiebericht Wege und Ansatzpunkte zur Verbesserung der Softwaresicherheit.

Die Zentren haben sich mit den Herausforderungen und Problemen der heutigen Softwareindustrie in Bezug auf IT-Sicherheit beschäftigt und Fragen aufgezeigt, die zur Verbesserung der Software als Wettbewerbsvorteil beantwortet werden müssen. Einige der Anregungen des Berichtes können unmittelbar gewinnbringend von der Softwareindustrie umgesetzt werden, andere brauchen noch industrielle Vorlaufforschung. Die perspektivischen Punkte müssen bei der Planung zukünftiger Forschungsprogramme von Fördergebern, von einschlägigen Forschungseinrichtungen und von Forschungsabteilungen der Softwareindustrie berücksichtigt werden.

Die Zentren wollen die Forschung maßgeblich vorantreiben und Partnerunternehmen unterstützen.

Der Trend- und Strategiebericht steht unter *www.sit.fraunhofer.de/secure-software-trends* zum Download bereit.

„Operation NetTraveler": Cyberspionage-Kampagne gegen regierungsnahe Organisationen und Forschungsinstitute

Kaspersky Lab veröffentlichte am 04.06.2013 Analyseergebnisse einer neuerlichen Cyberspionage-Kampagne[1]. Dabei wurde die Schadprogrammfamilie NetTraveler für APT-Attacken (Advanced Persistent Threat)[2] genutzt. Insgesamt wurden 350 hochrangige Opfer aus 40 Ländern kompromittiert. Die NetTravler-Gruppe infizierte Opfer aus verschiedenen Einrichtungen des privaten und öffentlichen Bereichs, unter anderem Regierungsinstitutionen, Botschaften, die Öl- und Gasindustrie, Forschungseinrichtungen, die Rüstungsindustrie sowie Aktivisten.

Aus dem Report von Kaspersky Lab geht hervor, dass die Angreifer bereits seit 2004 aktiv sind. Der Höhepunkt der Cyberspionage-Kampagne war zwischen 2010 und 2013. Die NetTraveler-Gruppe hat es in jüngster Zeit vor allem auf Informationen aus den Bereichen der Weltraumforschung, Nanotechnologie, Energieproduktion, Nuklearenergie, Lasertechnologie, Medizin und Kommunikation abgesehen.

1 http://www.securelist.com/en/blog/8105/NetTraveler_is_Running_Red_Star_APT_Attacks_Compromise_High_Profile_Victims

2 http://de.wikipedia.org/wiki/Advanced_Persistent_Threat