Entwicklungen erkennen

Das Zentrum für Infrastrukturelle Sicherheit der Donau-Universität Krems legt den Schwerpunkt darauf, Entwicklungen im Sicherheitsbereich frühzeitig zu erkennen und Antworten darauf zu finden.

Nicht Technikgläubigkeit wollen wir fördern, sondern Bewusstseinsbildung für Sicherheit betreiben“, sagte Dekan Prof. Dr. Walter Seböck, Leiter des *Instituts für Infrastrukturelle Sicherheit* bei der Eröffnung der 9. Sicherheitskonferenz am 27. Oktober 2011 in der Donau-Universität Krems. „Sicherheit ist eine Querschnittsmaterie. Wir wollen uns kontinuierlich mit aktuellen, die Sicherheit betreffenden Themen auseinandersetzen“.

Sicherheitskonferenz in Krems: Antworten auf aktuelle Sicherheitsfragen.

„Die Computer-Kriminalität verursacht weltweit 750 Milliarden Euro Schaden pro Jahr“, sagte General Franz Lang, Direktor des Bundeskriminalamts. „Mit einem Umsatz von 150 Milliarden übersteigt sie den des illegalen Drogenhandels. 150.000 Cyber-Angriffe werden pro Tag gezählt.“ Während sich in den 1990er-Jahren Freaks als Hacker betätigt hätten und es in der Szene als Erfolg gegolten habe, etwa den Webauftritt des Pentagons verändert zu haben, gehe es den Profis von heute entweder um großen Gewinn oder große Zerstörung.

„Wir müssen den Nutzern das Gefühl nehmen, gegen etwas Übermächtiges, gegen ein Phantom anzukämpfen, und Hilfestellung dort geben, wo sie gebraucht wird, beim Gewerbetreibenden oder dem potenziellen Opfer von Betrügereien, das Gefahr läuft, zwar zu zahlen, aber die bestellte Ware nicht zu erhalten“, forderte Lang. Es gelte, diejenigen zu erreichen, die aus Sachzwängen zur Technik gezwungen würden. Der Kontakt mit der Wirtschaft und der Wissenschaft werde gesucht: „Wir wollen wissen, was in den nächsten zwei oder drei Jahren auf den Markt kommt.“

Smartphones. FH-Prof. DI Grischa Schmiedl (FH St. Pölten) stellte die rhetorische Frage, wer sich bei Smartphones über deren Sicherheitseinstellungen und der von Web-Applikationen oder von Apps aus dem App-Store auskenne: „Der Nutzer hat nicht die geringste Ahnung und ist von den vielen Möglichkeiten frustriert.“ Die Konfigurationen seien zu komplex und für den User unverständlich.

Als Abhilfe schlägt Schmiedl das Konzept eines Trust-Centers vor, das angebotene Software überprüft und zertifiziert. Der Anwender solle beraten werden, welche Applikationen für seine Zwecke in Frage kommen, und bei der Vergabe von Rechten, die er der installierten Software einräumen will, unterstützt werden.

Mit der forensischen Untersuchung von Smartphones und welche Daten auf der SIM-Karte abgelegt sind und von dieser ausgelesen werden können, befassten sich Christopher Mallmann und Stefan Langeder (FH St. Pölten). DI (FH) Mag. Rainer Poisel (FH St. Pölten) stellte einen Vergleich her zwischen der Identifizierung von Schusswaffen anhand der charakteristischen Spuren auf dem Geschoß, mit den Daten, die bei der Aufnahme von Fotos, Videos oder Audiodateien entstehen. Digitalkameras generieren bei der Bildaufnahme spezifische Daten. Die verwendeten Color-Filter-Arrays lassen Rückschlüsse zu. Bei Audiodateien hinterlassen Charakteristiken des versorgenden Netzstroms forensisch verwertbare Spuren. Dazu kommt die Analyse des Bildinhalts, etwa, was die Umgebung betrifft, wo die Fotos oder Videos (Kinderpornografie) hergestellt wurden. Auch Inhaltsfälschungen von Bildern können erkannt und herausgearbeitet werden.

Franz Lang: „Wir wollen wissen, was in den nächsten Jahren auf den Markt kommt.“

Grischa Schmiedl: „Die Konfigurationen von Smartphones sind für den User unverständlich.“

Ing. Mag. Klaus Mak und DI Gerhard Backfried stellten die Arbeitsweise eines *Multimedia Documentation Labs* dar. Offene Quellen (Audio, Video; Internet; Social Media u. a.) werden ausgewertet und sprachlich sowie visuell so verarbeitet, dass weltweite Zusammenhänge erkennbar und über Suchfunktionen abrufbar werden.

Cloud Computing. Vor einigen Jahren bloß angedacht, ist Cloud Computing heute ein gängiges Betriebsmodell. Programme werden aus dem Internet bezogen und Daten dort gespeichert. Der Anwender erspart sich den Kauf teurer Hard- und Software. Im Prinzip genügt ein Laptop mit Internet-Anschluss.

Auf Probleme, die sich bei der Datenspeicherung „in der Wolke“ ergeben könnten, wies DI Martin Mulazzani von *Security-Research* hin. Auch Anbieter von Speicherdiensten müssen Speicherplatz sparen. Das geschieht dadurch, dass bestimmte, zahlreich wiederkehrende idente Datenmengen wie etwa Musikstücke nicht als solche, sondern bloß mit ihrem Fingerabdruck, dem „Hashwert“, gespeichert werden. Das bietet die Möglichkeit zu neuartigen Angriffen insofern, als ein unbe-

Fotos: Kurt Hickisch

Donauuniversität Krems: erste einzige staatliche postgraduale Weiterbildungs-Universität Österreichs.

rechtigter Datenzugriff möglich ist, wenn der „Hashwert" bekannt ist, ohne dass der Dienstleister oder das Opfer davon etwas bemerken. Wenn die Host-ID bekannt ist, können beliebige Daten abgespeichert werden, etwa kompromittierendes Material. Als Abhilfe eignet sich Daten verschlüsselt in die Cloud zur Speicherung zu übermitteln. Die erst dort von den Anbietern erfolgende Verschlüsselung reicht nicht aus, weil die Datenwege unsicher sind.

Wie Malware nach Klassen eingeteilt wird, erläuterte Dr. Otto Hellwig (FH St. Pölten). Derzeit stellen pdf-Dateien das am häufigsten benützte Transportmittel für Schadsoftware dar. Das Aufkommen von Spam geht zurück. Von 8 Milliarden täglich versendeten E-Mails sind 75 Prozent Spam.

Rolf von Rössing forderte, im Sicherheitsbereich den Menschen mehr in den Blickpunkt zu rücken. Anstatt ein Verhalten zu erzwingen, sollten durch Belohnungen Anreize geschaffen werden: „Prämien dann, wenn nichts passiert."

Kriminalität und Umfeld. Zwei Referenten befassten sich mit der Frage, inwieweit das bauliche Umfeld auf die Kriminalität Einfluss nimmt.

Mag. Birgit Zetinigg, B. A., MSc, vom Zentrum für Infrastrukturelle Sicherheit der Donau-Universität, präsentierte ihre Untersuchung, inwieweit gestalterische Elemente von Banken Einfluss darauf haben, ob ein Geldinstitut überfallen oder ein Bankraub unterlassen wird. Zu diesem Zweck analysierten sie 165 Banküberfälle, die zwischen Jänner 2002 und April 2007 begangen wurden, zunächst nach standardisierten Vorgaben. Von diesen Banken war im Untersuchungszeitraum die Hälfte schon vorher ein- oder mehrmals überfallen worden. Bei 18 Banken wurde an Ort und Stelle eine Raumanalyse durchgeführt.

Zudem wurden in acht österreichischen Justizanstalten 41 wegen Bankraubs verurteilte Straftäter, etwa 40 Prozent der im Untersuchungszeitraum wegen dieses Delikts in Haft befindlichen Personen, nach ihren Tatmotiven befragt und was nach ihrer Einschätzung von der Architektur des überfallenen Geldinstituts dem geplanten Überfall eher geeignet erschienen war oder was sie abgehalten hätte.

31 Prozent der Täter waren „Amateure", die Notsituationen (Spielschulden, Scheidung) zur Tat veranlasst hatten. Überfallen wurden von dieser Tätergruppe kleinere Banken in der näheren Umgebung, ohne großen Planungsaufwand und ohne Komplizen.

55 Prozent der Täter waren eher Gelegenheitstäter, hatten aber eine kriminelle Vergangenheit. Sie hatten in die Planung investiert, waren mit Komplizen unterwegs und großteils mit Schusswaffen bewaffnet.

Die „Profis" (14 %) waren von Komplizen begleitet, führten scharfe Schusswaffen mit und waren in der Planung „auf alles gefasst".

Je kleiner das Foyer und je näher die Kasse beim Ausgang ist, desto größer ist die Wahrscheinlichkeit eines Überfalls. „Zeit ist der wichtigste Faktor. Die Täter nehmen sich etwa zwei Minuten für den Überfall vor", erläuterte Zetinigg. Ferner verleitet eine offene Kassengestaltung geradezu dazu, dass sich der Täter durch Griff in die Kassenlade selbst bedient.

Auf 38 Prozent der Täter hatte es eine abschreckende Wirkung, wenn die Eingangstür elektrisch geschlossen werden konnte. 57 Prozent der Täter betrachteten es für die Tatausführung günstig, wenn sie durch Glasfassaden Einblick in das Innere der Kassenräume erlangen konnten. Dadurch war es ihnen möglich, Zeitpunkte abzuwarten, zu denen sich keine oder wenige Kunden im Kassenraum befunden hatten.

Auf 17 Prozent der Täter hatte eine Transparenz, die eine Beobachtung des Tatgeschehens von außen ermöglichte, eine abschreckende Wirkung. Für 14 Prozent waren beide Gesichtspunkte

FOTO: DONAUUNI KREMS/SUZY STÖCKL

DONAU-UNI KREMS

Security und Safety

Die 2001 gegründete Donau-Universität Krems (DUK) ist die erste und einzige staatliche postgraduale Weiterbildungs-Universität Österreichs. Das Zentrum für infrastrukturelle Sicherheit ist mit dem Zentrum für E-Governance, Teil des seit 1. Jänner 2011 eingerichteten Departments für E-Governance in Wirtschaft und Verwaltung und als solches Teil der Fakultät für Wirtschaft und Recht. Die Aspekte Security und Safety werden ganzheitlich erfasst, aus sozial-, rechts- und wirtschaftswissenschaftlicher sowie aus technischer Sicht. Entwicklungen werden national und international beobachtet. Die Ergebnisse fließen in angewandte Forschung ein und werden in berufsbegleitenden Lehrgängen und Seminaren vorgestellt. Das Durchschnittsalter der Lehrgangsteilnehmer liegt bei 40 Jahren. Sie bringen ihre bisherige Berufserfahrung ein. *www.donau-uni.ac.at*

Birgit Zetinigg: „Bauliche Maßnahmen können das Risiko von Banküberfällen verringern.“

Martin Mulazzani: „Daten sollen verschlüsselt in die Cloud zur Speicherung übermittelt werden.“

nicht von Bedeutung. Aus der Studie ergibt sich, dass bei Banken bauliche Maßnahmen geeignet sind, das Risiko von Überfällen zu verringern.

Der Zahlungsbereich sollte vom Servicebereich getrennt und die Kassen sollten möglichst weit weg vom Eingang sein. Beraterplätze sollten nicht von außen eingesehen werden können. Eine transparente Gestaltung empfiehlt sich, wo mit sozialer Kontrolle gerechnet werden kann, und bietet sich nicht an vor Haltestellen des öffentlichen Verkehrs.

Über den Zusammenhang zwischen Architektur und Kriminalität referierte auch Dr. Günter Stummvoll vom Department für Bauen und Umwelt der Donau-Universität. Als historische Beispiele führte er die Burgen des Mittelalters und Stadtmauern an. Nunmehr liege der Fokus auf dem Schutz des Einzelnen. Ein Merkmal der Sicherheitsgesellschaft sei die, durch Technisierung ermöglichte vorbeugende Kontrolle. Das öffentliche Leben verlagere sich in teilprivatisierte Räume, die eigene Hausregeln aufgestellt hätten.

Eine Raumpsychologie könne bei der Raumplanung und im Städtebau dazu beitragen, ein weniger kriminogenes Umfeld zu gestalten. Kahle Betonwände hätten einen negativen Einfluss auf das Sicherheitsempfinden. Bepflanzungen würden Graffiti hintanhalten. Auf Licht und Beleuchtung komme es an; warme Farben würden als angenehm empfunden. Obdachlose würden weniger ein Ärgernis darstellen, wenn am Morgen die Plätze, wo sie sich die Nacht über niedergelassen haben, wieder gesäubert werden würden. Stummvoll: „Sicherheit auch dort, wo nicht überwacht und kontrolliert wird.“

Kurt Hickisch

Fotos: Kurt Hickisch