

Forschung

Claudia Eckert: „Weil Angriffspläne sich mit hoher Dynamik ändern, müssen bessere Verfahren entwickelt werden, um Angriffe aus dem Internet früh zu erkennen.“ Die Leiterin des Fraunhofer Instituts für Sichere Informationstechnologie (SIT) spricht über Bedrohungen der IT-abhängigen Gesellschaft und die späte EU-Förderwelle für Informationstechnologie.

Die Spione kommen aus dem Netz

Christian Ellison

economy: Vor welchen Herausforderungen stehen Unternehmer heute im Bereich IT-Sicherheit?

Claudia Eckert: Größte Gefahren sehe ich durch Identitätsdiebstahl, verbunden mit dem Einschleusen von Spyware auf Rechnern, unterstützt durch die mangelhafte Sicherheit von Web-Diensten und Peer-to-Peer-Diensten (Anm. d. Red.: bei der Vernetzung von Rechnern via Internet, also Rechner-Rechner-Verbindung), hier insbesondere Voice over IP. Phishing ist eine

Ausprägung des Identitätsdiebstahls. Der klassische Ansatz, dies über Anhänge via E-Mails zu erreichen, ist allerdings überholt. Vermehrt haben wir es mit komplexeren Angriffsmustern zu tun – wie Cross Site Scripting, SQL-Injection –, die klassische Schwachstellen bei der Programmierung von Servern oder Diensten ausnutzen. Auf diesem Weg lassen sich unbemerkt Trojaner auf Rechner einschmuggeln, die etwa die Tastatureingabe abfangen – da wird die Passworteingabe bei einem Login mitverfolgt. So wird eine Verbindung zum Angreiferrech-

ner aufgebaut, um diese Daten zu übermitteln. Über eingeschmuggelte Spyware können dann Daten und Aktionen des Nutzers ausgespäht und an den Angreifer übermittelt werden. Im Namen des Nutzers können so Aktionen durchgeführt werden.

Wie wird das in der Zukunft ausschauen?

Wir werden nach wie vor damit kämpfen, dass kontinuierlich Angriffe auf die Systeme entwickelt werden, die es zu erkennen und abzuwehren gilt. Lösungen für allgegenwärtige Probleme werden in den Systemen integriert sein, sodass die Qualität der IT-Systeme verbessert wird. IT-Sicherheit ist ein Prozess und kein Systemzustand, die Fortentwicklung muss konsequent verfolgt werden. Da sich Angriffspläne mit hoher Dynamik ändern und ausgefeilter werden, müssen bessere Verfahren entwickelt werden, um Angriffe früh und mit hoher Treffergenauigkeit zu erkennen. Da wir noch abhängiger von IT sein werden, wird die Gesellschaft angreifbarer. Wir benötigen daher Methoden, um Systeme zu entwickeln, die sich selbst schützen, die sich eigenständig durch Umkonfigurierung „heilen“ können.

Sind das die Themen, mit denen Sie sich in der Forschung beschäftigen?

Ja. Wir denken aber bereits deutlich weiter. Zum Beispiel forschen wir nach den Umständen, wie in einer offenen, sich dynamisch verändernden Internet-Welt Vertrauensbeziehungen spontan, aber dennoch verlässlich etablieren, etwa in einer Peer-to-Peer-Umgebung, in der ich meine Partner nicht kenne, in der Partner beliebig viele unterschiedliche Identitäten annehmen können.

Ein anderer Bereich ist die Fahrzeug-zu-Fahrzeug-Kommunikation, bei der Fahrzeuge sich wechselseitig über Gefahrensituationen informieren. Angesichts des Vordringens von Informationstechnologie in alle Bereiche unseres täglichen Lebens, etwa RFID-Chips an und in Produkten wie Kleidung, suchen wir Antworten darauf, wie angesichts unzähliger digitaler Objekte, die mit meiner Person verknüpfbar sind und die es anderen erlauben, Profile über mich zu erstellen, Privatheit gewährleistet wird.

Haben Sie den Eindruck, dass die europäische Forschungspolitik der IT-Sicherheit die Bedeutung zuzmisst, die sie hat?

Im neuen, siebenten Rahmenprogramm der EU hat Sicherheit eine große Bedeutung. Ich sehe diese Entwicklung in der EU sehr positiv. Sie hätte schon etwas früher mit dieser Stärke einsetzen können. Aber wir starten nicht bei null. Auch in der

Steckbrief



Claudia Eckert ist unter anderem Professorin an der Technischen Universität Darmstadt. In Fachgremien wirkt sie an der Gestaltung der technischen und wissenschaftlichen Rahmenbedingungen in Deutschland sowie an der Ausgestaltung von wissenschaftlichen Förderprogrammen auf EU- und Nato-Ebene mit. Sie ist die einzige weibliche Institutsleiterin der Fraunhofer Gesellschaft. Foto: SIT

Vergangenheit wurden in der EU einige wichtige Sicherheitsthemen gefördert. Es muss klar sein, dass IT-Sicherheit auch in Zukunft ständig neuen Herausforderungen gegenüberstehen wird, sodass die Forschungsanstrengungen der EU sich nicht im siebenten Rahmenprogramm erschöpfen.

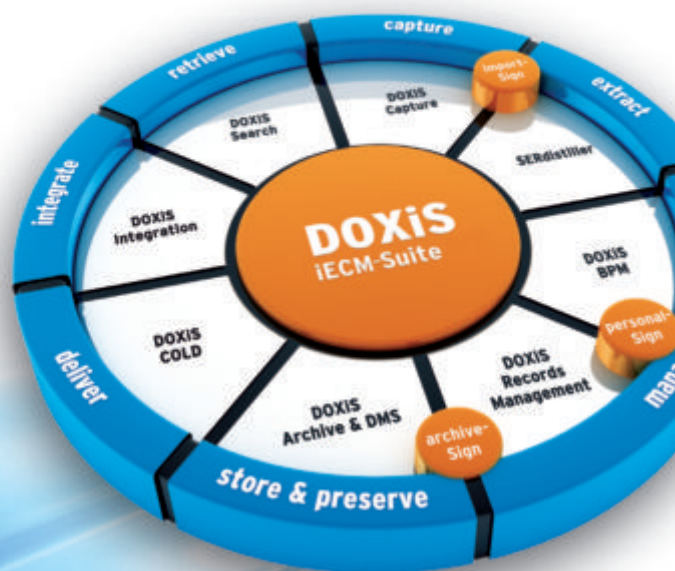
Welche Themen sind eigentlich gerade im Fraunhofer Institut von zentraler Bedeutung?

Generell unterstützt das SIT Unternehmen bei der Absicherung von Informationen, Geräten, Diensten und Netzen. Neben Sicherheitsstandards und Sicherheitstechnologien wie biometrischen Erkennungssystemen, digitalen Wasserzeichen oder Anwendungen der elektronischen Signatur beschäftigen wir uns damit, wie man IT nutzt, um die Sicherheit zu erhöhen. Aspekte sind hierbei der Schutz kritischer Infrastrukturen, aber auch die sichere Nutzung von IT im Auto und in Produktionsumgebungen oder der sichere Einsatz von Sensorsystemen wie RFID in Gebäuden. Hier haben wir mit Facilityboss eine Software entwickelt, mit der sich IT und Gebäudetechnik steuern und analysieren lassen. Zutritt zu Räumen, die Bewegungen von Personen und Objekten sowie der Zugriff auf sensitive Daten lassen sich so nicht nur ganzheitlich kontrollieren, sondern Unternehmen können mit diesem Werkzeug auch Prozesse im Gebäude effizienter gestalten.

www.sit.fraunhofer.de



Der Wettbewerbsvorteil integriertes Enterprise Content Management



- ▶ Hersteller und größtes unabhängiges deutsches Systemhaus für iECM
- ▶ Mehr als 2 Jahrzehnte Kompetenz und Erfahrung
- ▶ 1.000 Referenzprojekte europaweit
- ▶ ECM-Partner der Hälfte der DAX 30 Unternehmen
- ▶ 750.000 Anwender in allen Branchen

SER Solutions Österreich GmbH • Internet: www.ser.at • eMail: office@ser.at

DOXIS iECM-Suite - Fortschritt durch Produktivität

Im Fördertopf

Die Energieeffizienz von Gebäuden ist eine Schlüsselfrage im Hinblick auf Erreichung des Kyotoziels. Während im Neubau minimaler Energieverbrauch bereits Standard ist, gibt es beim Gebäudebestand größten Nachholbedarf. Mit dem Isover Energieeffizienz Award 2007 werden nun erstmals energetisch besonders erfolgreiche Modernisierungsprojekte ausgezeichnet. Der Award wird europaweit in zehn Ländern durchgeführt. Jedes Land wählt mit einer nationalen Jury seine Preisträger. Das Preisgeld in Österreich beträgt 30.000 Euro. Die Preisträger der nationalen Bewerbe werden im Rahmen der Batimat 2007 in Paris geehrt, ihre Wohnbauten in einem „Best of“-Buch präsentiert. Teilnehmen können Bauherren, Planer und ausführende Betriebe, die an einer Modernisierung unter Einsatz von Isover-Produkten beteiligt waren. Entscheidend ist, dass der Energieverbrauch des Gebäudes im Zuge der Modernisierung um zwei Drittel gesenkt und gleichzeitig das Wohnklima verbessert werden konnte. Die Modernisierung muss in den letzten sechs Jahren erfolgt sein, frühestens im Jahr 2000 – spätestens im Jahr 2006. Alle, die am Isover Energieeffizienz Award 2007 teilnehmen möchten, können sich bis spätestens 30. April 2007 unter www.isover.at anmelden. Die Einreichfrist endet am 30. Juni 2007. kl

