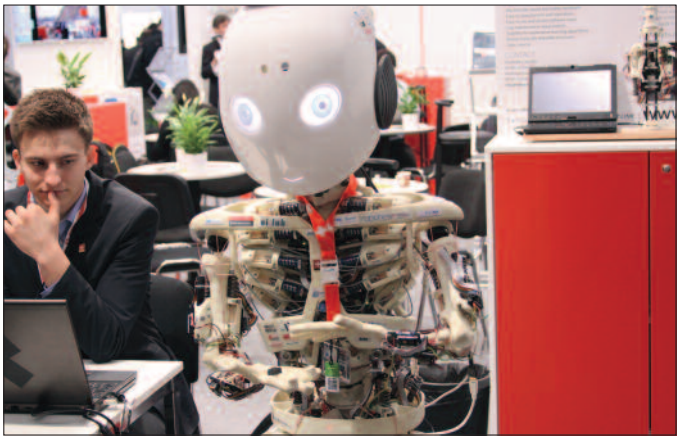
CeBIT 2014: Stand des Bundesamts für Sicherheit in der Informationstechnik (BSI).



Roboy: Humanoider Roboter mit künstlichen Muskeln und Sehnen und menschenähnlichen Eigenschaften.

Neue Produkte, neue Ideen

Die CeBIT 2014 präsentierte sich als Fachmesse für den Business-Bereich, mit einer Leistungsschau der IKT-Branche und einer Fülle von Informationen.

Von 2006 bis 2012 hat sich das weltweite Datenvolumen auf 2,5 Zettabytes verzehnfacht", sagte Bundesminister des Innern Dr. Thomas de Maiziére am 10. März 2014 bei der Eröffnung des *Public Sector Parks,* einem Teilbereich der *CeBIT 2014,* die vom 10. bis zum 14. März 2014 in Hannover stattfand. „Für 2020 wird ein Volumen von 40 Zettabytes vorausgesagt. Das ist eine Zahl mit 21 Nullen, und man fragt sich, wo der Nutzen dieser Unmenge von Daten liegt. Muss eigentlich wirklich alles aufgehoben werden?" Die Speichermassen müssten geordnet und kluge Anwendungen gefunden werden, im Straßenverkehr, in der öffentlichen Verwaltung, so, dass alle anderen davon Nutzen tragen. Datenschutz und Datensicherheit müssten durch Recht, Technik und eigene Vorsicht gewährleistet werden, betonte de Maiziére.

Die in Ausarbeitung befindliche Europäische Datenschutzverordnung müsse umsetzbar und anschlussfähig an das Internet sein. Beim Schutz durch Technik solle nicht auf den Angreifer abgestellt werden, sondern auf das, was zu schützen sei. Besondere Bedeutung komme dem Schutz kritischer Infrastruktur zu, betonte der Minister, und verwies darauf, dass in Deutschland noch in diesem Jahr ein IT-Sicherheitsgesetz erlassen werde.

BITKOM-Präsident Prof. Dieter Kempf wies darauf hin, dass 80 Prozent der Bevölkerung in Deutschland ein Smartphone bei sich hätten, bei der *Generation 60+* seien es knapp 60 Prozent. Über die Smartphones könnten Behördengänge abgewickelt werden. Die sichere Authentifikation könnte, ohne dass noch ein eigenes Lesegerät benötigt werden würde, berührungslos über den Chip des elektronischen Personalausweises abgewickelt werden, sofern diese Funktion vom Besitzer freigeschaltet wurde und das Smartphone NFC-fähig sei. Wie dies in der Praxis funktionieren könnte, wurde im *Public Sector Park* von der *Firma NXP (www.nxp.com)* anhand eines über das Handy gestellten Antrags auf Zuteilung eines Kinderbetreuungsplatzes demonstriert.

Nach dem am 1. August 2013 in Kraft getretenen Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz, EGovG) sollen die Bundesbehörden bis spätestens 2020 ihre Akten elektronisch führen. Papierdokumente sollen nach ihrer Übertragung in elektronische Dokumente vernichtet oder zurückgegeben werden.

Bedrohungslage. „Angesichts der Bedrohungen im Internet auf dieses einfach zu verzichten und zu Brief und Briefkasten zurückzukehren, geht einfach nicht mehr", sagte der Präsident des Bundesamtes für Sicherheit in der Informationstechnik *(BSI; www.bsi.bund.de),* Michael Hange. Zu vielfältig seien die Vernetzungen.

Die Cyber-Kriminalität folge den Gesetzen der Wirtschaft: Mit möglichst wenig Aufwand solle ein Maximum an Gewinn erzielt werden, betonte Dr. Dirk Häger vom *BSI*. Es gebe genügend Rechner, bei denen nicht einmal bekannte Schwachstellen behoben würden. 90 Prozent der Standard-Angriffe könnten mit Standard-Maßnahmen abgewendet werden. Von den häufigsten Schwachstellen, die weltweit im Jänner 2014 bei Angriffen durch Exploit-Kits detektiert wurden, gehen die Patches, mit denen die Sicherheitslücken geschlossen wurden, bis auf Mai/Juni 2012 zurück. Vom Bekanntwerden einer Schwachstelle bis zu deren Behebung vergehen etwa neun Wochen. Von 2010 bis 2013 wurden in häufig verwendeten Softwareprodukten täglich zwei neue kritische Schwachstellen entdeckt.

Schadprogramme werden nicht mehr hauptsächlich über Sex- und Pornoseiten oder über Anhänge zu E-Mails verbreitet. Als gefährlicher, weil unauffälliger, haben sich Werbebanner herausgestellt, durch deren Anklicken Schadprogramme auf den Rechner geladen werden. Derartige Drive-by-Exploits tragen zu 40 Prozent zur Verbreitung von Malware bei, direkter Download über eine URL zu 30 Prozent und E-Mail-Anhänge zu 20 Prozent. Der Rest von 10 Prozent entfällt auf Infektionsquellen wie Datenträger.

FOTOS: KURT HICKISCH

Fast drei Prozent der deutschen Websites sind als gefährlich anzusehen. Stark im Steigen begriffen ist die Zahl der Malware-Programme für mobile Geräte. Derzeit sind etwa zwei Millionen solcher Programme bekannt.

Die Zahl der Botnetze wird weltweit auf 1.150 geschätzt. Man geht davon aus, dass in Deutschland rund eine Million Rechner in derartige Netze eingebunden sind. „Rent a Bot“: 10.000 Bots kosten 160 Dollar. Botnetze sind ein lukratives Universalwerkzeug. Sie können zum Bitcoin-Mining eingesetzt werden, zu DDos-Angriffen, um andere Rechner lahmzulegen, zu Informations- oder Identitätsdiebstahl, Klickbetrug, Ransomware und Spamversand. Die durchschnittliche Angriffsbandbreite bei DDos-Angriffen beträgt in Deutschland etwa 2,5 Gbit/sec, doch wurden bereits Angriffe beobachtet,

Dirk Häger: „Die Cyber-Kriminalität folgt den Gesetzen der Wirtschaft.“

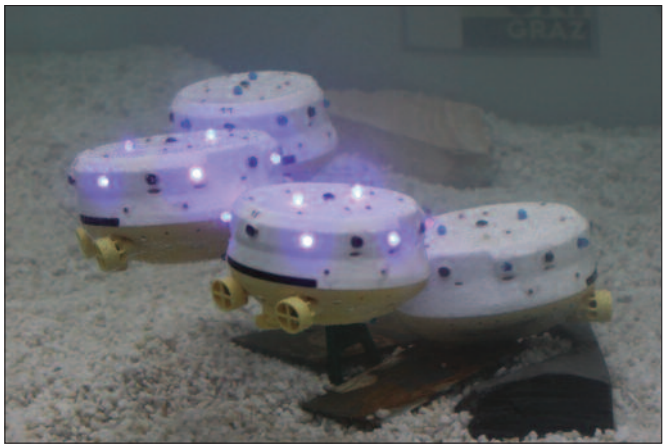
die mit 400 Gbit/sec gefahren wurden. Ein DDos-Angriff dauert durchschnittlich 30 Minuten. Einen solchen Angriff in Auftrag zu geben, kostet für eine Stunde 5 Dollar, für einen Tag 100 Dollar. Nach den Erkenntnissen des *BSI* erfolgen in Deutschland pro Tag mindestens zehn DDos-Angriffe auf Wirtschaftsunternehmen und Behörden, insgesamt waren es

Michael Hange: „Man kann auf das Internet trotz Bedrohungen nicht verzichten.“

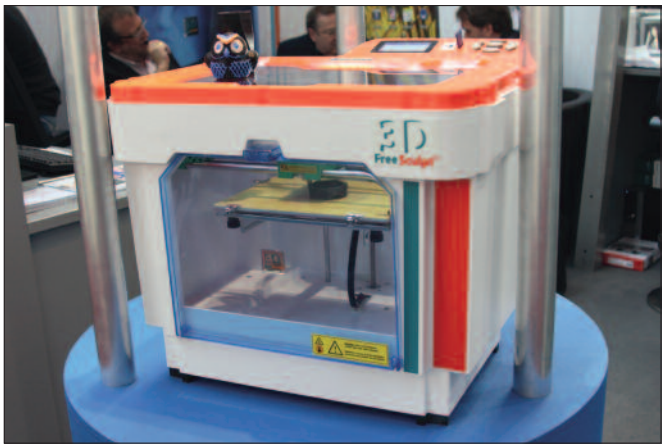
2.200 im Jahr 2013. Zu 53 Prozent betreffen die Angriffe E-Commerce, zu 20 Prozent E-Sport, zu neun Prozent Blogs/Content. Motive sind unter anderem politisch-ideologische Auseinandersetzungen, Betrug beim Online-Gaming und Vandalismus. Gezielte Cyber-Spionage-Angriffe *(Advanced Persistant Threat)* werden durchschnittlich erst nach etwa acht Monaten entdeckt, und zwar zu zwei Drittel durch Hinweise von Außenstehenden, wie etwa Polizeibehörden. Zielgruppen sind Rüstungsindustrie, Automobilbau, Schiffsbau, Raumfahrt, Forschungseinrichtungen und die öffentliche Verwaltung. Die Angreifer arbeiten arbeitsteilig und teilweise hoch professionell; sie sind gut ausgestattet. „Praktisch jedes Unternehmen wird attackiert, nicht alle merken es“, betonte Häger.

Die Allianz für Cyber-Sicherheit *(www.allianz-fuer-cybersicherheit.de)* nimmt Meldungen über Cyber-Attacken entgegen und leitet sie mit vom BSI beigesteuerten Sicherheitsempfehlungen an alle Mitglieder weiter. Der Allianz sind bisher über 700 Unternehmen beigetreten, wöchentlich kommen fünf bis zehn dazu. 75 Firmen sind Partner und etwa 27 Multiplikatoren verteilen die

Fotos: Kurt Hickisch



Unterwasserroboter: Sie könnten Giftmüll oder versunkene Flugschreiber aufspüren.



3D-Drucker für den Heimbereich: Kunststoff wird über eine Düse geschmolzen und Schicht für Schicht aufgetragen.

Produkte und Informationen sowie das Know-how der Partner.

Innovative Produkte. *Secunet (www.secunet.com)* hat ein Tablet mit hardware basierter Vollverschlüsselung der Festplatte entwickelt. Die Authentisierung erfolgt über einen externen Stick. Wird dieser vom Gerät abgezogen, ist der Rechner gesperrt und kann nur wieder durch Anstecken desselben Sticks wieder aktiviert werden.

Globe Flight (www.globe-flight.de) hat Multikopter („Drohnen“) vorgeführt, die etwa 25 Minuten in der Luft bleiben können und während dieser Zeit über die eingebaute Kamera Videos in Full-HD-Qualität liefern. Die Einsatzmöglichkeiten solcher Drohnen durch Beobachtung aus der Luft sind vielfältig. Im Schwarm können sie auch zur Suche eingesetzt werden.

Die Universität Graz *(http://cocoro.uni-graz.at)* präsentierte kleine Unterwasserroboter, die Giftmüll oder versunkene Flugschreiber aufspüren könnten. Mehrere kleine Roboter sind billiger und effektiver als ein einzelnes, großes und teures Spürgerät.

Etliche Unternehmen haben 3D-Drucker für den Heimbereich angeboten, in einer Preisklasse von etwa 800 bis 2.500 Euro. Ein als „Draht“ von einer Rolle gelieferter Kunststoff wird über eine Düse (Extruder) bei etwa 230 Grad geschmolzen und programmgesteuert Schicht für Schicht aufgetragen. Die Anwendungsmöglichkeiten dieser additiven Fertigung von Gegenständen werden auch im Consumer-Bereich ständig erweitert und gehen über die spielerische Erprobung dieser Technologie hinaus *(www.Thingiverse.com)*. So wurden Beispiele aus der Architektur gezeigt: Geschäfts- und Büroinnenräume in verkleinertem Maßstab als 3D-Modell, ebenso Häuser *(3yourmind; www.3yd.de)*.

Einige Firmen *(IGO3D GmbH; www.igo3d.com)* liefern Kameras für 3D-Aufnahmen (3D-Scanner) mit, aus denen die Rechenprogramme erstellt werden können. *Fabmaker (www.fabmaker.com)* bietet ein Ausbildungsprogramm für Schulen an, einschließlich einem Drucker, der die heiße Abluft filtert und ähnlich einem Backrohr allseitig geschlossen ist, um versehentliches Hineingreifen und damit Verbrennungen zu verhindern.

Projekte. Die Polizei Baden-Württemberg hat ein Simulationsprojekt mit virtuellen Trainingsszenarien entwickelt, das für die Schulung von Einsatzsituationen verwendet werden kann. 150 km² Stadtgebiet werden virtuell dargestellt, in dem sich ein Polizist als Spielfigur (Avatar) frei bewegen kann, zu Fuß oder im Streifenwagen. Ihm werden Einsatzsituationen eingespielt, auf die er zu reagieren hat, bis zur Anforderung der Unterstützung durch einen Hubschrauber. Die virtuellen Szenarien werden dort eingesetzt, wo die reale Übung zu aufwendig, zu teuer oder zu gefährlich wäre. Das Pilotprojekt läuft derzeit in drei Dienststellen in Stuttgart.

Ein Beispiel für E-Government stellt die in Nordrhein-Westfalen und Baden-Württemberg bereits eingeführte Online-Sicherheitsüberprüfung (OSiP) dar. In Verfahren, bei denen die Zuverlässigkeit überprüft werden muss (Waffen-, Sprengstoff-, Luftsicherheitsrecht) werden die Informationen automatisiert elektronisch und weitgehend medienbruchfrei aus den Datenbanken abgerufen. Verfahren werden so rascher erledigt, und Mitarbeiter entlastet.

Das *Zentrum für satellitengestützte Kriseninformation (ZKI)* in Pfaffenhofen, Bayern *(www.zki.dlr.de)* bietet Satellitendaten zur Bewältigung von Katastrophen an, etwa bei Hochwasser. Anhand der Geodaten (Topografie) ist es auch möglich, die Folgen beispielsweise eines Dammbruchs an einer bestimmten Stelle sowie den zeitlichen Ablauf der Überflutung der betroffenen Gebiete im Vorhinein zu berechnen und grafisch auf einer Landkarte darzustellen.

Der Verein „White IT e.V.“ *(www.whiteit.de)* ist als gemeinnütziger Verein ein Dachverband von etwa 60 Organisationen, die gegen den Missbrauch von Kindern in der Gesellschaft auftreten. Die Geschäftsstelle wird beim Niedersächsischen Ministerium für Inneres und Sport geführt. Der Verein präsentierte auf der CeBIT unter anderem kindgerecht gestaltete Flyer sowie eine „Vereinbarung über die Internetbenutzung“ zwischen Kind und Erziehungsberechtigtem, mit „10 Goldenen Regeln“, deren Einhaltung zugesichert wird. Ein Wettbewerb über die besten Ideen zum Schutz von Kindern („Kinderhände sagen JA!“) läuft bis 30. September 2014. Unter *www.juuuport.de* finden Jugendliche eine Online-Beratung zu mit dem Internet in Zusammenhang stehenden Themen.

Mehr als 210.000 Besucher kamen zur *CeBIT 2014*, die als Business-Messe für Fachbesucher ausgerichtet war. Die nächste *CeBIT* wird vom 16. bis 20. März 2015 in Hannover abgehalten.

Kurt Hickisch

Fotos: Kurt Hickisch