

## Absatz-Boom bei Daimler hält an

**STUTTGART.** Der Autobauer Daimler gibt Gas. Im Oktober wurden mit 108.400 Fahrzeugen der Marken Mercedes-Benz, Smart, AMG und Maybach elf Prozent mehr verkauft als im Vorjahr, wie Mercedes-Vertriebschef Joachim Schmidt gestern in Stuttgart mitteilte. Die Kernmarke Mercedes-Benz legte um knapp 14 Prozent auf 100.500 Wagen zu. „Wir sind mit einem kräftigen Plus ins vierte Quartal gestartet und konnten im Oktober zum zwölften Mal in Folge unseren Absatz im zweistelligen Prozentbereich steigern“, sagte Schmidt. „Unser Erfolg auf dem deutschen Markt war maßgeblich an der Entwicklung beteiligt.“ Auf dem Heimatmarkt verbuchten die Stuttgarter ein Absatzplus von 14 Prozent auf 27.000 Fahrzeuge. Die deutlichsten Steigerungen wurden aber erneut in China erzielt, wo die Auslieferungen auf 13.500 Autos mehr als verdoppelt wurden. Sorgenkind von Daimler bleibt weiter der Kleinwagen Smart: Um über 15 Prozent auf 7.900 City-Flitzer sackte der Absatz ab. lsw

## ZF erweitert in Saarbrücken

**FRIEDRICHSHAFEN.** Der Autozulieferer ZF Friedrichshafen erweitert seine Produktionsanlagen in Saarbrücken. Wegen der starken Nachfrage nach 8-Gang-Automat-Getrieben soll bis zum Frühjahr 2012 eine zusätzliche 8.000 Quadratmeter große Halle gebaut werden, teilte der drittgrößte deutsche Autozulieferer gestern in Friedrichshafen am Bodensee mit. „Nach Ende der Wirtschaftskrise hat die Nachfrage nach unseren Pkw-Getrieben so stark angezogen, dass wir unsere Produktionskapazität früher als geplant ausbauen“, sagte ZF-Chef Hans-Georg Härter. dpa

# Nicht nur Würmer sind gefährlich

Computer-Hacker Sebastian Schreiber gibt beim Kongress der Pforzheimer Firma ITML Kostproben seines Könnens

**PFORZHEIM.** Kriege werden künftig nicht mehr mit Panzern und Raketen geführt, sondern mit Bits und Bytes. Doch auch Firmen und Privatleute werden vermehrt angegriffen, warnt Computer-Experte Sebastian Schreiber.

PZ-REDAKTEUR  
LOTHAR H. NEFF

Der professionelle Hacker – seine Tübinger Firma SySS GmbH testet im Kundenauftrag deren Computernetze – demonstrierte beim ITML-Forum in Mannheim, wie man solche Angriffe ausführt. Die Einsatzgebiete sind vielfältig: Da installiert Schreiber kurzerhand einen Trojaner auf einem Handy eines Vortragsteilnehmers, knackt den Barcode einer Supermarktkette oder bedient sich per Online-Banking an einem fremden Girokonto. Selbst speziell gesicherte Laptops oder Speicherchips mit geheimen Daten sind für den Hacker kein großes Problem.

Zwölf Attacken in einer Stunde präsentiert Schreiber den staunenden Gästen der Pforzheimer Firma ITML – Partner des Software-Riesen SAP. Auch in mehreren Fernsehsendungen zeigte der Tübinger schon sein Können, da war beispielsweise die Sparkasse Leipzig ein Ziel seiner Angriffe. Wenn ihm die Lederwaren in einem Onlineshop zu teuer sind, reduziert er kurzerhand den Preis. Auch beim Computerspiel „Moorhuhn“ trägt er sich raschmal mit dem Bestwert von 2500 Punkten in die Siegerliste ein. Eine weitere Spezialität sind viren-infizierte PDF-Dateien als



Knackt Netzwerke: Sebastian Schreiber.

Foto: privat

E-Mail-Anhang, die dann das Kommando im Rechner übernehmen.

Mit dem Computervirus Stuxnet, der unlängst die Schaltsysteme iranischer Atomanlagen erreichte, hat Schreiber freilich nichts zu tun. Wer steckt hinter der rätselhaften Attacke? Für Schreiber ist klar, dass es sich beim Stuxnet-Wurm um eine po-

tentielle Kriegswaffe handelt, der aber vermutlich versehentlich freigesetzt wurde. Dabei handelt es sich um den ersten Wurm, der Industriesysteme nicht nur ausspionieren, sondern auch deren Funktionsweise manipulieren kann. Was ihn stutzig macht, ist, dass kein Amateur-Hacker hinter dem Virus steckt, son-

dern gezielt bis zu zwei Millionen US-Dollar in die Entwicklung gesteckt worden seien. „Verbreitet wurde Stuxnet wohl über einen infizierten Computer-Stick“, glaubt Schreiber. Urheber könnte ein ausländischer Geheimdienst oder ein Wettbewerber von Siemens gewesen sein. Der Münchner Konzern, auf dessen Steuerungen bei industriellen Kunden Stuxnet bislang aktiv wurde, spielt den Vorfall herunter. Doch es gibt genügend eindrückliche Horrorszenerarien: totaler Stromausfall, der Verkehr in Großstädten bricht zusammen. Giftgas entweicht aus Chemiefabriken, Züge entgleisen, Satelliten und Flugzeuge stürzen ab. Bei Siemens hält man den Ball flach: 15 Fälle von Infektionen sind dem Konzern bekannt – bislang ohne Folgen,

erklärt Tino Hildebrand, Leiter Marketing & Promotion Simatic bei Siemens Industry Automation auf Anfrage der Fachzeitung Produktion: In keinem der Fälle war die Steuerung der Anlage beeinträchtigt. „Seit Ende August wurde kein neuer Fall gemeldet.“

An den teils wilden Spekulationen zum Thema Stuxnet will Siemens sich nicht beteiligen. Klar ist dem Konzern aber auch, dass es sich bei dem Wurm nicht um die zufällige Entwicklung handeln kann. „Vielmehr müssen der oder die Urheber neben IT-Kenntnissen auch spezifisches Know-how über industrielle Produktionsprozesse gehabt haben“, sagt Hildebrand.

@ www.SySS.de

## „Feindliche Übernahme“

Internet-Kriminalität mit Hilfe sogenannter Botnetze ist weltweit auf dem Vormarsch. Immer häufiger werden diese Netzwerke aus gekaperten Computern für die Verbreitung von schädlicher Software verwendet, um zum Beispiel an Kontodaten zu gelangen.

Europaweit rangierte Deutschland beim Botnet-Befall auf dem vierten Platz hinter Spanien, Frankreich und England. Weltweit von den kriminellen Attacken am meisten betroffen ist Südkorea, ermittelten Forscher von Microsoft. Hier wurden im Zeitraum zwischen Januar und Juni 14,6 Infektionen pro 1000 überprüfte Computer registriert. Nach absoluten Zahlen waren die USA Spitzenreiter mit 2,2 Millionen Infektionen,

Brasilien folgte mit deutlichem Abstand mit 550.000 Ansteckungen. In Europa fallen in Spanien mit 382.000 Infektionen die meisten privaten oder gewerblich genutzten Rechner einer „feindlichen Übernahme“ zum Opfer.

In Deutschland am weitesten verbreitet ist der Studie zufolge die Botnetz-Familie „Alureon“, sie macht rund 30 Prozent aller bekannten Botnetze aus. Mit inzwischen acht Prozent folgt darauf die das Botnetzwerk „Rimecud“. Die Hälfte der Betreiber sensibler Netzwerke etwa aus Energiebranche, Gesundheits- oder Bankenwesen, die schon einmal Ziel einer Attacke waren, vermutet eher politische Gründe hinter den Cyber-Angriffen. dpa

Anzeige

Es ist wieder so weit! 1500,- Euro für die Besten!

# CLUB DER JUNGEN DICHTER

Einsendeschluss:  
28. Februar 2011

SCHREIBWETTBEWERB  
FÜR SCHÜLER/INNEN



Altersgruppe  
10 bis 13 Jahre

Mein bester Freund,  
meine beste Freundin

oder Was mir Mut macht

Altersgruppe  
14 bis 16 Jahre

Ich lebe gerne hier, weil...

oder Was mir Mut macht

Mitmachen lohnt sich...

Den beiden Kategorie-Siegern winkt ein Geldpreis von je **1500 Euro**. Für die Zweitplatzierten gibt es je **750 Euro**, für die Drittplatzierten ein **S-Club-Sparkonto** bei der Sparkasse Pforzheim Calw mit je **250 Euro**. Weitere zehn Texte werden mit **Buchpreisen à 20 Euro** belohnt. Gestiftet von der Buchhandlung Thalia. Die Schule mit den meisten Einsendungen erhält zugunsten der Schulbücherei **500 Euro**, gestiftet von der Baden Württembergischen Bank.

Und nun: denkt nach, schreibt auf – es lohnt sich! Die Wettbewerbsbeiträge müssen folgende Angaben enthalten\*) damit sie für die Auswertung weiter bearbeitet werden können: Name, Adresse, Telefon, Alter, Thema.

Anzahl der Worte: (10 – 13 Jahren) **maximal 600 Worte** – (14 – 16 Jahren) **maximal 1000 Worte**

Die Texte schickt Ihr an **Jakob- und Rosa-Esslinger-Stiftung** – Poststraße 5 – 75172 Pforzheim oder per E-Mail an **dichter10@pz-news.de** (Gruppe 10 – 13 Jahren) – **dichter14@pz-news.de** (Gruppe 14 – 16 Jahren)

\* Wer eine Geschichte einsendet, erklärt sich damit einverstanden, dass die PZ frei und kostenlos darüber verfügen kann (insbesondere Adressen in der Zeitung). Sie/er erklärt damit auch, dass die Geschichte nirgendwo abgeschrieben oder nachgezogen ist. Aus organisatorischen Gründen können wir die Texte nicht zurückschicken.