

IT-MESSE CEBIT 2014 Vom Daten sammeln, auswerten – und schützen

Zugriff im Netz

Das Internet wird zur Datenkrake. Wie man Informationen vor unerwünschten Nutzern bewahrt, ist Thema des Branchentreffs

VON CORINNA VISSER

Was nützt das sicherste Vorhängeschloss und die beste Alarmanlage, wenn die Hintertür offensteht? Nichts. Hintertüren gibt es aber nicht nur an Gebäuden, sondern auch bei Software. Sie ermöglichen es Angreifern, unter Umgehung der normalen Sicherheitsschranken auf fremde Computer zuzugreifen. Hintertüren werden manchmal zu Servicezwecken eingerichtet, oft sind es einfach nur Programmierfehler. Das perfride daran: „Meist merkt der Angreiffene nicht einmal, dass seine Technik kompromittiert wurde“, sagt Ralf Koenzen, Geschäftsführer des Netzwerkspezialisten Lancom. Die Sicherheit von Netzen und Daten wird eines der großen Themen auf der IT-Messe Cebit sein, die an diesem Montag in Hannover beginnt.

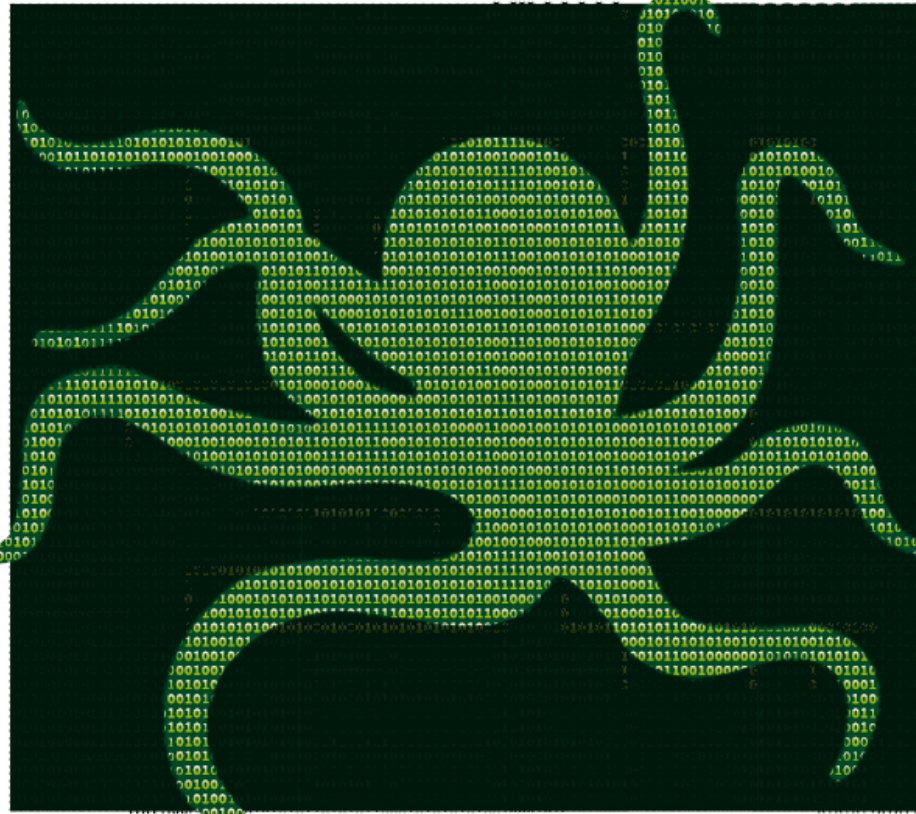
„Datability“ haben sich die Veranstalter als Leitthema der Messe ausgedacht, ein Kunstwort, das die beiden Megatrends der digitalen Welt – die wachsende Datenmenge und den verantwortungsvollen Umgang damit – zusammenfassen soll. So geht der US-Marktforscher IDC davon aus, dass die weltweit gespeicherte Datenmenge von 2,8 Billionen Gigabyte im Jahr 2012 auf 40 Billionen Gigabyte bis 2020 anwachsen wird.

Zugleich werden die Methoden, diese riesigen Datenmengen in Echtzeit zu analysieren, rasant weiterentwickelt. Dabei geht es nicht nur um Unternehmensdaten, sondern zum Beispiel auch um Ge-

sundheitsinformationen, Verkehrsdaten oder die Informationsströme zwischen Maschinen. Der Markt für „Big Data“ soll 2014 allein in Deutschland auf 6,2 Milliarden Euro wachsen, prognostiziert der Branchenverband Bitkom.

Das Netz wird zur Datenkrake. Doch je mehr Daten in großen Datenspeichern (Cloud) gespeichert und übers Netz zugänglich sind, desto mehr haben auch die Enthüllungen von Edward Snowden gezeigt, wie wichtig es ist, die Sicherheitsstandards ebenfalls weiterzuentwickeln. „Big Data bedeutet auch: Angreifer können heute auf eine Schnittstelle zugehen, an der zahlreiche Daten aggregiert sind. Sie müssen nicht mehr viele einzelne Ziele im Unternehmen angreifen“, stellt Alexander Geschonneck von der Beratungsgesellschaft KPMG klar. Nach seiner Beobachtung passiert am meisten dort, wo viele Kundendaten zu finden sind: im Handel, bei Versicherungen, Anbietern von Internetdiensten, Finanzdienstleistern oder Telekommunikationsbetreibern – aber auch bei Behörden. „Angreifer haben es vornehmlich auf persönliche Daten, Postadressen, Mails und Zahlungsinformationen abgesehen“, sagt Geschonneck. „Vor Edward Snowden haben wir zwar gewusst, dass solche Angriffe möglich sind“, sagt Lancom-Geschäftsführer Koenzen. „Jetzt wissen wir, dass alles, was technisch möglich ist, auch gemacht wird.“

Wobei Koenzen überzeugt ist, dass Unternehmen primär von Cyber-Kriminalität bedroht werden und diese Angriffe von Kriminellen noch weitaus gefährlicher seien, als vom US-Geheimdienst NSA ausspioniert zu werden. Und tatsächlich berichtet Geschonneck von KPMG: „Unsere Beschäftigung als Ermittler im Bereich Cybercrime ist in den vergangenen sechs Monaten massiv angestiegen.“ Ein Einfallstor für Angriffe sind die Router, also die Geräte, die die Verbindung zum Internet herstellen. Drei Hersteller gibt es noch in Deutschland, wobei Lancom und Bintel-Elmeg Produkte für Unternehmen anbieten, AVM (Fritzbox) für Privatkunden. Marktführer im Geschäftskundenmarkt ist allerdings der US-Konzern Cisco. Lancoms Router sind jedoch als einzige vom Bundesamt für Sicherheit in der Informationstechnik zertifiziert für ihre „Hochsicherheit gegen Abhören, Manipulation und Sabotage“. Das Softwarehaus Datev nutzt die Router, um mehr als 7000 Steuerberater sicher ins

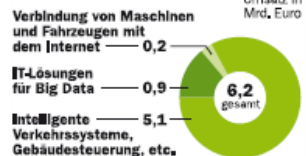


Großes Wachstum bei Big Data

Der Markt für Big-Data-Lösungen in Deutschland



Der Big-Data-Markt 2014 gliedert sich in drei Segmente



Quelle: Bitkom

Top/Infot4

Netz zu bringen. Möglich sei dies, weil alle Komponenten in Deutschland hergestellt und auch die Software eine komplette Eigenentwicklung sei, sagt Koenzen. „Bei uns gibt es garantiert keine Hintertür“, verspricht er. Über die Geschäftsentwicklung könne er sich nicht beklagen. Im vergangenen Jahr sei der Umsatz um 18 Prozent gewachsen. „Der Markt für Sicherheitstechnik steht noch am Anfang“, sagt Koenzen. Zwar wurden viele Geschäftsführer durch die Snowden-Enthüllungen aufgeschreckt. Doch es dauert, bis Entscheidungen fallen – und kostet Geld.

Auch die Entwicklung der Produkte kostet Zeit. So kündigte die Telekom-Tochter T-Systems bereits im November einen IT-Sicherheitsdienst namens „Clean Pipe“ an, mit dem kleine und mittelständische Firmen sowie öffentliche Verwaltungen sicher ins Netz kommen sollen. Das Sicherheitsniveau soll dem eines Großunternehmens entsprechen, wobei der gesamte aus- und eingehende Verkehr verschlüsselt und nach außen abgeschirmt an ein deutsches Cloud-Rechenzentrum von T-Systems geleitet werde. Zum Paket gehört dabei der hochsichere Router von Lancom.

Doch statt einer fertigen Lösung zeigt T-Systems auf der Cebit Prototypen und Pilotprojekte. Der Marktstart soll allerdings „noch im Laufe des Jahres“ erfolgen, heißt es.

Koenzen hält den Wandel der Cebit zur reinen Fachmesse für richtig. „Für uns ist die Messe eine wichtige Kontaktbörse mit unseren Fachhändlern und Kunden“, sagt der Lancom-Geschäftsführer. „Der Terminkalender ist voll.“ Auch die Aufmerksamkeit der Politik hält er für wichtig. „Sie kann dafür sorgen, dass in kritischen Anwendungen vertrauenswürdige Geräte eingesetzt werden“, sagt er.