IBM

IBM DB2 Universal Database: providing privacy and security for customer information

Highlights

Provides authentication, authorization, privileges and security

Supports fair information practices

Complements IBM privacy consulting services

Building consumer trust in e-business interactions

From an enterprise point of view, e-business focuses on transforming business processes, expanding market reach, improving price/performance and creating new business opportunities. But from a market-oriented perspective, e-business is really all about customers. The most successful e-businesses are those that understand their customers and know how to meet their needs.

Leveraging the power of customer information gathered through e-business interactions, companies can execute business intelligence programs that provide a precise portrait of their customers' wants, needs and buying patterns. Such profiles enable companies to attract and retain the most profitable customers.

However, customers' attitudes — and hence loyalty — are greatly affected by their confidence in how the company will use their personal information. Protecting the privacy of that information must be a central consideration in any e-business implementation. And it is impossible to manage information privacy without good security. Organization-wide security processes and products enable information systems to address confidentiality, integrity and availability risks.

As part of IBM's comprehensive security offerings, IBM DB2® is designed to provide the highest level of security possible in a relational database management system, while leveraging the security features of the hardware platforms on which it operates.

e-business

For instance, DB2 optionally invokes the IBM SecureWay® Security Server for OS/390® (RACF®) to perform access control checking.

DB2 security features

DB2 security provides capabilities in four key areas: authentication, authorization, privileges and integrity.

Authentication is the process of identifying a person logging in as a user or as a member of a group. DB2 interfaces with the authentication system of the operating system on which it is running and supports all four industry-accepted authentication methods: trusted client, client encrypt, server and DCE.

Authorization involves determining which functions users are allowed to perform. Users can be authorized to perform a group of functions, ranging from system authorization, which allows all functions, to lower levels, such as the ability to execute the high-speed LOAD utility.

Privileges constitute a finer level of security control, such as the ability to view a table or modify it. If a privilege is on a view, then it only applies to the subset of the table represented by this view. Combined with the USER special register, this allows the user to work with privileges at a row level in a table.

DB2 also supports the RUN privilege, which enables users to run the application but not to change the SQL statements of that application. This enforces additional security since the user cannot issue any SQL statements other than the one in the application.

Integrity is the ability to control relationships between data. Integrity involves referential integrity, check constraint and triggers:

- Referential integrity (RI) can be used to enforce the relationship between tables. Fox example, an order cannot exist for a customer number if that number does not exist in the customer table.

- Check constraint is the ability to enforce some rules on a column of a table, such as 'salary cannot be > $200,000.'

- Triggers provide the ability to enforce rules other than RI between tables, such as 'customer cannot be on a mailing list if it is flagged for mailing list exclusion in the customer table.'

DB2 supports fair information practices

Responsible information handling relates to the way an organization collects and uses personally identifiable consumer information. This includes any information relating to an identified or identifiable person.

DB2 supports fair information handling by upholding the following principles:

Notice/awareness. The existence of systems containing personally identifiable consumer information should be publicly known along with the uses of that information. Clear notice concerning the types of information being collected and the purposes for its collection and use can be given to consumers any time personal information is collected.

DB2 supports openness by enabling automatic consumer notification when personal data — such as address or information use permission — is added or changed. When such information is first entered into the database, an insert trigger defined on the DB2 contact information table is activated to notify the consumer. When existing information is changed, the update trigger is similarly activated.

Choice/consent. Information should be used only for purposes specified at the time of collection, and not be sold, exchanged or otherwise communicated to external users without the consumer's consent. DB2 enables protection of information use through the DB2 AUDIT facility and DB2 Opt-In/Opt-Out tables.

The security provided by DB2 views ensures that people only have access to the information that they need to access. Further, the DB2 AUDIT facility can capture all requests made by an agent for audit purposes. The information from the DB2 audit trace can be stored in the database and queried if fraud is suspected or if individuals wish to know how their information was used.

Access. Consumers should have the right to see data about themselves and to correct any information that is not accurate, timely, relevant or complete. DB2 enables verification of accuracy through DB2 views, encryption and DB2 user-defined functions (UDFs).

Enforcement/recourse. Mechanisms should be in place to assure compliance with policies and appropriate recourse should be available to an injured party when policies are not followed. Using the DB2 AUDIT facility, you can track all accesses to and uses of consumer personal information to ensure quality and integrity (all requests are captured and kept in the database).

Security/information quality and integrity. Companies should keep only that personal data which is relevant for the defined purposes, consistent with principles of awareness and choice. To the extent necessary for these purposes, the data should be accurate, complete and current. Companies should keep a record of how personal information has been used. DB2 interfaces with Hierarchical Storage Manager to allow data to be migrated to tape and recalled automatically.

IBM privacy implementation model

With its privacy consulting services, IBM helps businesses understand and address the growing number of issues about protecting the privacy of personal data online. IBM also helps create and enable effective, proactive strategies that address these issues.

A unique tool-assisted methodology at the core of IBM's privacy consulting services delivers a clear plan for privacy readiness. This methodology shows the steps involved and the questions that need to be addressed to set up the right privacy policies and systems.

"The fact that IBM has institutionalized its privacy intellectual capital into a tool means that the company can identify both the hard costs such as new systems and upgrades, but also the 'soft' costs that many potential customers didn't even consider."

–Ellen Carney, Director and Principal Analyst, Dataquest

The two core elements of IBM's privacy consulting services are a privacy workshop and privacy strategy and implementation services.

The privacy workshop helps decision makers identify strategies for responsible handling of customer information. It also defines management action plans. Such strategies enable companies to provide Web-based services that meet their customers' privacy expectations in concert with applicable laws and regulations.

Privacy strategy and implementation services help businesses develop and implement an effective consumer and employee privacy strategy. The resulting implementation can help define an effective privacy policy, addressing issues such as e-business, data warehousing, data mining and customer relationships. An additional aspect of this service presents ways to position a company for increased customer satisfaction and competitive advantage.

IBM security and privacy consulting is part of IBM's broad range of e-business security services, which help companies worldwide build and maintain secure information systems. IBM offers its customers proven technologies and innovative, widely accepted security solutions for the rapidly changing computing environment.

This includes tailoring privacy requirements for specific industry regulations and customer needs. IBM's focus on secure information management, coupled with a commitment to privacy, can lead to stronger, more beneficial relationships between companies and their customers.

For more information

Contact your IBM marketing representative or IBM authorized software reseller or visit our Web site at *www.ibm.com/security.*

IBM Corporation
Santa Teresa Laboratory
555 Bailey Avenue
San Jose, CA 95141

Produced in the United States of America
02-00