PHYS.ORG

IBM attacks the complexity of security with identity intelligence

January 12 2012

IBM announced a new identity intelligence breakthrough designed in IBM labs to provide corporations with a far more sophisticated approach to managing the information employees can access.

An employee's unauthorized access to client information can leave a firm vulnerable to security breaches and audits. Many companies juggle the administration of identifying, managing and approving employee access, some of whom have roles that require different levels of access to financial, personnel or sales and customer data, and can change during the course of a year.

To meet that challenge, IBM is unveiling advanced analytics software called Security Role and Policy Modeler. Based on IBM Research innovation, the software analyzes employee data and recommends a finite set of roles to better secure an organization and manage compliance. The analytics can flag abnormal behavior, inconsistencies in role access and expired user access.

For example, a 10,000-employee hospital may allow administrators only to have certified access to financial and human resource systems. Their access must be revoked as their roles change within the organization. The Security Role and Policy Modeler evaluates all 10,000 user identities across the hospital and narrows those down to 100 roles such as 'administrator.' This reduces costs and complexity to manage security.

"With the rise of cloud and mobile access, it's no surprise that identity management has become such a hot button to clients," said Marc van Zadelhoff, vice president strategy and product management, IBM Security Systems. "If an organization doesn't know who has access to their data, how can meet compliance regulations, let alone be secure? Today's news shows how IBM is applying its advanced intelligence to solve the most complex security issues."

Bharti Airtel and Cognizant Tap IBM's New Software

Bharti Airtel, the top telecommunications provider in India, and Cognizant, an IT consulting and business process outsourcing in the U.S., are already seeing the benefits of the new software.

"The new IBM offering will provide greater insight to our role modeling and lifecycle management that is so critical to allowing our employees, partners and third parties to securely access data they are authorized to," said Felix Mohan, Global Chief Information Security Officer, Bharti Airtel. "Using the intelligence and automation of the Role and Policy Modeler, we can manage our identity and roles much more efficiently and effectively."

"One of the first steps of a secure enterprise is knowing what your own employees have access to," said Barry Miracle, director of Digital Security, Cognizant. With IBM's new identity management software, I will have better insight across the company into roles and identities of who is accessing particular applications or databases, making our compliance reporting more efficient."

Security Role and Policy Modeler is now available as part of IBM's software for policy-based identity and access management governance offering. The new software allows companies to efficiently collect, clean up, correlate, certify, and report on identity and access configurations. Specific new functions include:

· Scoring metrics and analytics that give business users the ability to produce a more effective role and access structure. Users can be identified by specific role they play in an organization. For example, a marketing team manager can only allow employees to access marketshare data but not human resources information.

· Clearer view into the role structure —such as organizational hierarchy charts, and access exceptions due to business needs -- that can be managed throughout the users' lifecycle. For example, if an employee moves from one department or function to another, that employee can be assigned--or restricted from--accessing particular applications or business assets based on their role structure within the organization.

· Single web-based interface to create, apply and validate roles that have multiple members. For example, a "physician" can be the group role and "cardiologist" or "radiologist" is the member role. Each role can be assigned different access and can be mined to identify outlying behavior and validated for violations.

IBM today also announced today announced that it set a new U.S. patent record in 2011, marking the 19th consecutive year that the company has led the annual list of patent recipients. IBM inventors earned a record 6,180 U.S. patents in 2011, including more than 100 security-related patents, adding to more than 3,000 patents in IBM's security portfolio. The 2011 patents granted include advances in identity intelligence for authenticating user identity when resetting passwords, verifying personal identity and detecting fingerprint spoofing.

Provided by IBM

Citation: IBM attacks the complexity of security with identity intelligence (2012, January 12) retrieved 17 May 2024 from https://phys.org/news/2012-01-ibm-complexity-identity-intelligence.html