Stay ahead of insider threats with predictive, intelligent security

Identifying and mitigating insider threats in the age of big data

Contents

Today organizations are faced with protecting data and applications against external and internal threats across a complex security landscape. According to the Kroll Annual Global Fraud Report, a recent survey that polled more than 1,200 senior executives worldwide, 2011 figures show that 60 percent of frauds are committed by insiders, up from 55 percent last year.[1] Modern trends in enterprise computing, the rise of social media, the cloud, mobility and the era of big data are making insider threats harder to identify, and giving insiders more ways to pass protected information to outsiders with less chance of discovery.

Security intelligence can help combat insider threats amid the digital information explosion. IBM has the ability to identify and protect against internal threats through a distinctive combination of robust foundational controls and intelligent reporting and management tools. Our solutions can help you protect valuable business assets, foster secure and efficient collaboration, and effectively integrate security into existing business processes.

The evolution of insider threats

In the past, insider threats typically referred to an employee with privileged access to sensitive or private data that could accidentally or deliberately alter that information or give it to an inappropriate recipient. Digital collaboration, mobility and social business have expanded the insider threat to include employees, contractors, consultants and even partners and service providers. Today we see three categories of insider threat:

- Trusted unwitting insiders—employees with privileged access that unwittingly expose sensitive data
- Trusted witting insiders—privileged employees that purposely expose private data to an external party
- Untrusted insiders—unauthorized users who have assumed the identity of a trusted insider

Trusted unwitting insider threats are unintentional. Careless employees may ignore strong password policies, leaving their laptop open to a malicious actor. IT managers could mishandle offsite backup tapes and inadvertently expose sensitive company information. Database administrators may accidentally expand read/write permissions to database tables, forget to patch a database vulnerability or use default system settings and configurations. But even the unintentional actions of trusted unwitting insiders have serious consequences when it comes to the theft or exposure of precious corporate assets such as revenue figures, trade secrets, intellectual property, sensitive negotiations and customer information.

The trusted witting insider has malicious intent to alter or steal data. These individuals may be motivated by greed or resentment or could be the victims of extortion. Thumb drives, the explosion of data on enterprise networks, and increases in mobility and social media make it easier for privileged users to extract sensitive information without detection.

The untrusted insider threats are the most difficult to discern and give malicious individuals privileged access to your data and systems. These adversaries take advantage of compromised or stolen user credentials, backdoors and malware to masquerade as trusted users behind your firewall and other perimeter defenses.

According to the 2011 Cyber Security Watch Survey, 33 percent of respondents view insider attacks to be more costly than external threats, compared to 25 percent in 2010.[2] With added dimensions to the insider threat and the boundaries of IT infrastructure being extended or altogether obliterated, security intelligence must inform your technical controls, security policies and user education.

Intelligent security systems to combat insider threats

Internal threats are difficult to identify and eradicate because they manifest as privileged users performing legitimate functions. Armed with deep business insight, advanced security research and sophisticated technology, you can take an intelligent approach to combating insider threats with foundational security elements, including:

- Data protection
- Privileged user monitoring
- Identity and access management
- Data redaction
- Security intelligence and analytics

Securing the flow of data

The move to new platforms including cloud, virtualization, mobile and social business makes it hard to secure the flow of data. Your trusted users can access applications from anywhere and they continue to blur the lines between personal and professional use of devices and data. Enterprises need a 360-degree strategy for protecting diverse types of data, including structured and unstructured, online and offline, and within development and test environments. Data protection to combat internal threats should include:

- Database vulnerability assessment
- Database activity monitoring and access prevention
- Access monitoring for file shares
- Data encryption
- Automated data discovery

Security intelligence and analytics can evaluate the effectiveness of your data protection technologies. They can also correlate large amounts of security event data to isolate anomalies and identify patterns of insider abuse.

Monitoring privileged users

User activity monitoring is a critical part of active defense against insider threats. The 2010 Verizon Data Breach Investigations Report notes that "insiders were at least three times more likely to steal intellectual property than outsiders."[3] But organizations often lack the security intelligence needed to link insiders to malicious behavior. A privileged user activity monitoring solution establishes baseline patterns of activity

for each user, and then creates alerts when anomalous behavior is observed, certain applications/systems are accessed, or unusual volumes of data are sent or received. Based on security intelligence, user activity monitoring solutions provide comprehensive visibility into user activity and its impact. This technology collects and correlates not only log data, but also Layer 7 network flows, asset data, configuration information and vulnerability data to identify pre-threat exposures and compromised employee accounts.

Apparel company detects insider data theft

User activity monitoring from IBM helped a large apparel company discover the insider theft of sensitive intellectual property. By correlating database access (via logs) with employee email transmissions (via flows) and comparing this activity against the employee's "baseline" activity, the solution was able to identify anomalous behavior indicative of an insider threat. As a result, the company identified the employee and stopped the action before the theft was complete.

Managing identities and access for secure collaboration

In the face of insider threats, protecting valuable data and resources takes more than a simple user ID and password. You need strong authentication that relies on sound policy for identity assurance. This helps not only protect against the bad guys; it also eliminates opportunities for negligent insiders to unintentionally leak data and helps prevent insider threats that originate from lax deprovisioning of expired or orphan accounts.

Identity and access management (IAM) solutions should help classify users by roles and access requirements and set policies for automated user life cycle and password management. Role-based policies make it easier to manage exceptions and identify abuse that could signal an insider threat. IAM solutions should also perform monitoring and enforcement to help identify policy violations. It is not enough to simply allow or deny access to applications; you must know who is requesting access and why, and what an individual is doing with access rights once they are received.

Enhancing security with intelligence and analytics

Even with the foundational security controls needed to protect against malicious internal attacks—authentication systems, asset tracking and data protection software, device and Internet usage monitoring, and more—it remains difficult to detect insiders performing legitimate functions from a legitimate place. Security intelligence provides a better understanding of the steady state, so you can recognize actions that deviate from expected boundaries such as number of connections, data transmitted and requested transactions.

Security intelligence also helps detect insider threats occurring over an extended time period. IBM uses security intelligence to focus on specific events, assets or transaction types to store and analyze a much smaller and more manageable amount of data. This makes it possible to identify even a "low and slow" attack from the inside.

It is more difficult to recover from an insider attack because insiders use their privileged access to clean up the systems they've attacked and eliminate their tracks. Security intelligence and analytics solutions keep a forensic activity trail at the intelligence hub, away from the actual systems that are being compromised. This facilitates identification of the attacker and simplifies clean up.

IBM security intelligence and analytics enable communication, correlation and analysis at a granular level across a wide range of security components, including authentication gateways, physical security systems, asset management tools, data protection technology, network monitoring capabilities, database monitoring and web security platforms. One reason organizations find it difficult to detect insider attacks is the time it takes to analyze a vast amount of data coming from a wide array of devices, entry points and user accounts. Consider how much more powerful and streamlined your insider threat detection capabilities can become when events are correlated across the IT environment.

Conclusion

It has become more important, yet more difficult, to secure critical information and related assets from insider threats. IT complexity is the leading cause of increasing fraud exposure, cited by 36 percent of 2011 Kroll Annual Global Fraud Report respondents compared with 28 percent last year. Developing *security intelligence*—the ability to proactively predict, identify and react to potential threats—is a top priority. IBM offers foundational security controls, and security intelligence and analytics to address the full spectrum of insider threats. We can help you assess your current risk to insider attacks and develop a strategic, prioritized approach to prevention across the extended enterprise.

For more information

To learn more about IBM Security, please contact your IBM marketing representative or IBM Business Partner, or visit the following website: **ibm.com**/security

Additionally, IBM Global Financing can help you acquire the IT solutions that your business needs in the most cost-effective and strategic way possible. We'll partner with credit qualified clients to customize an IT financing solution to suit your business goals, enable effective cash management, and improve your total cost of ownership. IBM Global Financing is your smartest choice to fund critical IT investments and propel your business forward. For more information, visit: **ibm.com**/financing

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
December 2011

[1] Source: "Most Fraud is an Inside Job, Says Survey"; CSO Magazine; Nov. 9, 2011.

[2] Source: CERT- http://www.cert.org/insider_threat

[3] http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

Please Recycle

WGE03014-USEN-00