Stay ahead of insider threats with predictive, intelligent security

Identifying and mitigating insider threats in the age of big data

Contents

2 The evolution of insider threats

2 Intelligent security systems to combat insider threats

3 Enhancing security with intelligence and analytics

4 Conclusion

Today's organizations are faced with the challenge of adequately protecting data and applications against numerous threats across a complex security landscape. However, few threats pose a greater danger than insider threats, especially those from privileged users. With unfettered access to sensitive assets—and often able to delete any trace of their activities—privileged users can wreak havoc on the unsuspecting enterprise.

Meanwhile, administrators often lack the right tools to deal with insider threats. In fact, according to a recent study, 88 percent of IT operations and security managers polled recognized insider threats as a cause for alarm, but admitted having difficulty identifying specific threatening actions by insiders. Also, 42 percent of respondents were not confident that they have the enterprise-wide visibility for user access.[1]

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 across the extended enterprise. IBM solutions can help identify and protect against internal threats through a distinctive combination of robust foundational controls and intelligent reporting and management tools.

The evolution of insider threats

In the past, insider threats typically referred to an employee with privileged access to sensitive or private data who could accidentally or deliberately alter that information or give it to an inappropriate recipient. With trends such as outsourcing and moving applications and data to the cloud, the insider threat can now 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 who unwittingly expose sensitive data
- Trusted witting insiders—malicious employees who 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, but they can have serious consequences when it comes to the theft or exposure of precious corporate assets such as revenue figures, intellectual property and customer information.

The trusted witting insider, on the other hand, 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, 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, back doors and malware to masquerade as trusted users behind your firewall and other defenses.

When it comes to preventing advanced insider threats, having a layered defense that leverages multiple technologies is vital. IBM offers various security solutions to help organizations set up entitlements, protect and monitor user access, and provide security intelligence to highlight inappropriate activities.

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 and auditing
- 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. 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 and auditing privileged users

User activity monitoring and reporting is a critical part of active defense against insider threats and a key requirement for security compliance. But organizations often lack the security intelligence needed to link insiders to malicious behavior. A privileged user activity monitoring and auditing solution is vital to establishing baseline patterns of activity for each user, and then creating 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.

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 not only helps 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.

Healthcare provider secures patient and employee data

A worldwide family of healthcare clinics required a sophisticated identity management system to easily manage and protect digital identities of hospital employees and patients. In addition, the organization needed easy integration within its complex IT system and simplified compliance management tools to demonstrate compliance with security regulations. IBM® Security Privileged Identity Manager helped the clinic control and monitor system administrator access to IT resources, helping protect the privacy of sensitive patient data.

Identity and access management (IAM) solutions should help classify users by roles and access requirements and set governance policies for automated user recertifications, lifecycle management and password management. 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, 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 cleanup.

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. 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 solutions, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
February 2015

IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at **ibm.com**/legal/copytrade.shtml

This document is current as of the initial date of publication and may be changed by IBM at any time. It is the user’s responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

[1] “Privileged User Abuse & The Insider Threat,” a survey of 693 IT operations and security managers, *Ponemon Institute*, June 2014.

Please Recycle