Closing the Intelligence Gap with Identity-Powered Security

Security Magazine | Travis Greene | February 10, 2014

Something has gone horribly wrong in the world of security.

While security investment has continued at a steady pace, so have devastating data breaches – and the future trends don't look any better. Yet, perplexingly, we continue to behave as though simply spending more money and devoting more resources to what has failed in the past will yield a different result in the future.

In no other part of the business would such an approach be acceptable or tolerated.

The challenge is that for the security industry, any advances in keeping data safe are almost immediately offset by equivalent advances in the skills and tools of the attackers. Worse, the very ground on which security is built – the infrastructure of business computing – is undergoing convulsive change, driven by cloud, mobility and social media. Even treading water has become an all but unattainable goal.

So how does the security industry move past the spiral of chasing after new magic cure-alls while watching success drift even further away? The answer is to broaden the use of information sources to better inform the security processes we already have.

The most basic question that any security team must answer revolves around the concept of what is "normal." Is the behavior of this system, this service, or this person "normal" and "safe?" Or is what we are seeing an indication of suspicious or malicious behavior? The ability to answer this question, with what is termed "security intelligence," is fundamental to understanding whether your organization is under attack. So much that it would be easy to imagine the capability to answer it is commonplace. It isn't.

Instead, organizations often struggle to understand who people really are, let alone whether they are behaving in a way that might suggest they were an insider with intent to damage, or perhaps that an outsider has compromised a privileged account.

This identity challenge – understanding who a user is, what is normal for them, what access they need, and what is business-appropriate for them fuels the security intelligence gap we continue to fail to close.

Another contributing factor to our intelligence gap is lack of monitoring and management of privileged users who have overly broad access rights to systems and data. As a result, organizations continue to experience avoidable data breaches, compliance failures and unnecessary risk. Worse, when a privileged account is compromised and used as a vector for an attack – or that privileged user decides to behave maliciously – it's often difficult to determine what they are doing and why.

Organizations must integrate "identity" into their security practices so that users with inappropriate access rights can be identified, monitored and managed to avoid unnecessary risk from internal and external attackers.

> *"2014 needs to be the year security teams begin to embrace the notion that deeper identity context is required to improve security and incident response.". "*

Travis Greene

Far too often, identity is relegated to operational tasks like provisioning access to business tools. Yet your "identity" carries invaluable information that could enrich and inform security teams who need to understand whether your access to a sensitive database is part of your job, or part of a plan to steal from your employer.

As more and more of the computing environment moves out of the control of the corporate IT function – out into the cloud or onto mobile devices – so too has the need to integrate a deep understanding of who the user really is, and what is normal for them becomes a foundational part of effective security monitoring.

Integrating identity into security monitoring will empower security teams to cut through the noise of activity and quickly identify if what they are seeing is normal and acceptable, or unusual and damaging. For example, when an employee exhibits unusual behavior, such as accessing a sensitive data store from a remote location on a mobile device rather than the usual method from the office, security teams can appropriately respond.

2014 needs to be the year security teams begin to embrace the notion that deeper identity context is required to improve security and incident response. This is the year for "identity-powered" security that provides the deeper identity context through integration with security monitoring to meet the demands of our complex and changing security landscape, closing the intelligence gap.

Without such identity-powered security, the fact is that we are going to see security teams continue to struggle to understand what behavior they are seeing, and most importantly, what the events they are monitoring really mean – and that is ultimately a recipe for continued failure, and more and more damaging data breaches.

Travis Greene is a Sr. Solution Strategist, Identity Management at NetIQ.

SECURITY
SOLUTIONS FOR ENTERPRISE SECURITY LEADERS

http://www.securitymagazine.com/articles/85222-closing-the-intelligence-gap-with-identity-powered-security