Executive Brief

Four Best Practices for Pragmatic Data Security

www.stealthbits.com | 201-447-9300

Identify Threats. Secure data. Reduce risk.

STEALTHbits TECHNOLOGIES

Four Best Practices for Pragmatic Data Security

Data security is a major issue for any company that has valuable information to protect. Breaches of that data can cost an organization dearly in the form of business disruption, loss of revenue, fines, lawsuits, and perhaps worst of all, the loss of trust between the organization and its customers and partners. But the challenge of securing all that data is daunting, and it's easy to lose sight of the fact that some small changes can have a major impact. Just as a journey of a thousand miles starts with one step, you have to break it down. The pragmatic approach to data security is to focus on the highest risk areas that can be solved with the least amount of effort. So, where do you start?

Let's start by looking at some facts.

- 95% of the Fortune 1000 use Active Directory (Microsoft)
- 80% of data is unstructured data (CSC)
- Authentication-based attacks factored into four of every five breaches involving hacking (2012 Verizon DBIR)

Even if you extend beyond the Fortune 1000, Active Directory is the clear market leader in the directory services space. Active Directory is the keys to the kingdom as the authentication and authorization hub of virtually every organization's IT infrastructure. Given that 80% of the data within any organization resides in unstructured form on File Shares, SharePoint Sites, and laptops, the vast majority of an organization's data is secured by Active Directory. So it's no wonder that four of every five breaches involving hacking leveraged techniques to compromise Active Directory itself.

So, again, where do you start? Start with Active Directory and your unstructured data.

By following these four pragmatic best practices for data security, organizations can quickly reduce the risk of data breaches and all their disastrous consequences.

1. Close Down Open Access

There are some legitimate reasons why every single person in your organization should have access to a resource, but those reasons are few and far between. Understanding where open access conditions exist and remediating them can have an immediate and dramatic effect on your organization's security posture.

Reducing open access also reduces your risk exposure by enforcing least privilege access concepts, and when taking the process a step further by assigning data custodians and performing regular entitlement reviews, also enables IT to transfer accountability for data to the data owners themselves.

2. Monitor Activity

Monitoring activity is an essential capability, but be careful not to bite off more than you can chew. The best way to make effective use of your monitoring efforts is to focus on specific scenarios you'd like to detect. For instance, not every change in Active Directory is critical. In fact, most aren't. However, the following changes and activities are the most important to be aware of at all times.

- Modifications to sensitive security groups that supply access to sensitive data or large numbers of systems
- User account creations and deletions, password changes, successful logons, and user lockouts
- Privileged account usage and authentications
- Creations, deletions, and modifications to any and all Group Policy Objects
- Access changes and access activities within known sensitive data locations

Monitoring these specific activities will prove much more effective than monitoring everything and trying to sift through the noise later.

3. Detect Abnormal Authentication Activity

One of the richest sources of security intelligence has been within your reach for quite some time. Yet few know how to leverage it properly. The vast majority of your Active Directory security logs are filled with the thousands or even millions of authentication events being handled by Active Directory every day. Being able to harness this data and pick out patterns of behavior from it is difficult, but infinitely useful when done right. Would you expect to see a single user attempt to authenticate to 200 systems in your environment in a 2 minute time period? Probably not. This is a prime example of malware infection and propagation using stolen credentials obtained using techniques like Pass the Hash and Pass the Ticket.

Being able to detect the following patterns of behavior will enable you to understand you're under attack now, in time to do something about it.

- X failed logins against any single host in Y minutes (Brute Force Attack)
- Successful or failed authentications of a given account across X number of resources in Y minutes (Horizontal/Lateral Account Movement)
- X number of failed login attempts from an individual user account in Y minutes (Account Hacking)
- Successful authentication after repeated failures (Breached Password)
- X number of logins from multiple systems within Y minutes (Concurrent Logins)

4. Locate Your Sensitive Data

How can you protect your sensitive data if you don't even know where it is? Determining what you consider sensitive, and then pinpointing the locations of that information allows you to plan your response. The most common options are to move the data to safer locations, encrypt the data in place, verify systems containing sensitive data are patched properly and up to date with the latest anti-virus definitions, classify the data, or even delete the data if it is no longer needed. The bottom line is that if there is nothing there to steal, then you're that much more secure.

To learn more about how STEALTHbits can help you employ these powerful, pragmatic approaches to data security, contact us today.

About STEALTHbits Technologies, Inc.

Identify threats. Secure Data. Reduce Risk.

STEALTHbits is a data security software company. We help organizations ensure the right people have the right access to the right information. By giving our customers insight into who has access and ownership of their unstructured data, and protecting against malicious access, we reduce security risk, fulfill compliance requirements and decrease operations expense.

Learn More

Attend a Demo - http://www.stealthbits.com/events

Browse the Resource Library - http://www.stealthbits.com/resources

Ask us a Question - http://www.stealthbits.com/company/contact-us

Request a Free Trial - http://www.stealthbits.com/free-trial

Visit the Official STEALTHbits Blog - http://www.stealthbits.com/blog

STEALTHbits Technologies, Inc.
200 Central Avenue
Hawthorne, NJ 07506
P: 1.201.447.9300 | F: 1.201.447.1818
sales@stealthbits.com | support@stealthbits.com
www.stealthbits.com

EB-PADS-0615