Case Study

University of BRISTOL

Implementing Real-Time Database Activity Monitoring at the University of Bristol

Key business drivers and deployment experience

> *"We knew we needed to do more to secure our databases. We chose Hedgehog as we could install it quickly and easily & unlike network-based solutions, it protects us against all types of attacks."*
>
> - Cameron Capewell
> DBA

Version 1.0, February 2010

Provided by

sentrigo™

www.sentrigo.com

Background

Like many educational institutions, the University of Bristol has both an extremely open environment and a highly dynamic user base, creating unique challenges for IT security. With more than 20,000 students attending each year, plus an additional 5,000 staff & faculty positions, the annual turnover of new and graduating students, along with guest faculty, warrants significant attention when it comes to securing sensitive data.

The University of Bristol implemented Sentrigo Hedgehog Enterprise (a real-time Database Activity Monitoring and breach preventions suite) and vPatch (Virtual Patching solution) in 2009, providing a greater degree of protection for personally identifiable information of its applicants, students, faculty, staff and alumni, as well as for the University's financial, academic, and research data.

About University of Bristol

- One of the top 10 Universities in the UK
- More than 20,000 students and 5,000 faculty / staff
- Undergraduate, post-graduate, and research activities across 6 disciplines
    - Arts, Engineering, Medical and Veterinary Sciences, Medicine and Dentistry, Science, and Social Sciences & Law

The Need for Greater Security

With the arrival of a new information security officer in 2008, the University tasked each of its academic computing teams with evaluating their current security postures, and identifying vulnerabilities and potential solutions in light of greater threats from external hackers or malicious insiders. While the University was not aware of any specific data leaks in the past, the frequent announcements of data breaches at other universities across the globe suggested that a more secure environment was nonetheless advisable.

The University of Bristol utilizes a range of different applications and databases, storing and processing data in support of virtually all operations at the school from Human Resources and Financials, to student grades and research projects. Many of these systems contain sensitive data, and after conducting a detailed analysis the team identified several common areas for improvement:

- Extending database audit to all systems, allowing the University to trace every access to be certain data has not been compromised.
- Log analysis was being done regularly, however for the most critical data more immediate alerting or active intrusion prevention could be beneficial.
- More visibility into the activities of privileged users (including system administrators, developers, and DBAs), and separation of duties, would provide greater oversight.
- While database patches issued by the vendors were applied to most systems soon after release, for a small number of applicactions the inability to schedule downtime, or application compatibility issues, delayed some updates.

Databases and Sensitive Information

- More than 30 production databases, plus an additional 40+ for training / development
- Multiple versions of both Oracle and Microsoft SQL Server
- Many databases subject to strict access control and/or containing private data:
    - Names, identification numbers
    - Financial information: aid applications, scholarships, grants
    - Grades, transcripts, test results, etc.
    - Research data and other intellectual property

Getting Started

As part of the database team's due diligence Cameron Capewell, one of just three DBAs that support more than 70 databases, attended a course on database security offered by the SANS institute. While the processes in place at Bristol were generally in line with best practices at the time, it was clear that the sophistication of attacks within the hacking community was increasing rapidly, and, Cameron remembers, "we knew there was a lot more we could do."

The first step was to conduct a comprehensive vulnerability assessment, so as to build a complete picture of what databases were in place, identify those containing sensitive data as well as which applications were utilizing those data, and determine the general security status of each system (patch level, priveleged accounts, et cetera). After a thorough review of a range of different solutions, the team concluded that getting better information about database activity, and utilizing intrusion detection and prevention techniques, could significantly reduce the risk of a breach.

The question was then: what technologies to use? And from which vendors? To best answer these questions, a project board was formedwith representation from the database team, the database "customers" in various applications groups, and the end-user community itself. The goal was to implement much stronger controls without creating obstacles to smooth data access for authorized use.

Choosing the Best Solution

After reviewing products from several different vendors, the team selected Sentrigo's Hedgehog Enterprise for database activity monitoring and Hedgehog vPatch to protect unpatched systems. With the relatively small team it was crucial that, whichever solution they picked, it must be easy to deploy. As with almost every educational institution today, there were significant constraints on budget as well; Sentrigo's software-only solution could be run on existing systems, significantly reducing costs.

The most influential factor in selecting a product was ultimately whether it would **best meet the security goals of the University**. It was in this area that Sentrigo set itself apart. The unique architecture, based on autonomous sensors on each server, provided protection from and immediate reaction to all threats. As Cameron stated, "We looked at other database activity monitoring solutions, and we chose Hedgehog based on the way it monitors memory, so we can prevent breaches before they occur. And unlike network-based solutions, Sentrigo sees all types of attacks, even from priveleged users."

Furthermore, Cameron added, "We try to always apply Oracle CPUs [Critical Patch Updates] and Microsoft patches as soon as possible, but it's not always easy to negotiate the downtime for that. 'Virtual patching' allows us to protect against vulnerabilities addressed in the Oracle CPUs within a more realistic timeframe. So, now it buys us some time, because with the virtual patches we know that we are safe until a point when we can actually apply the update."

On Selecting Sentrigo

> *"We looked at other database activity monitoring and auditing solutions, and we chose Hedgehog based on the way it monitors memory – so we can prevent breaches before they occur. And unlike network-based solutions, Sentrigo sees all types of attacks, even from privileged users."*

On Implementing Hedgehog

> *"Hedgehog has been just incredibly easy to deploy. I think it was about a half an hour to install the server… then each sensor took about 5 minutes… **that's been brilliant, really."***

- Cameron Capewell
DBA, University of Bristol

Up & Running Quickly

One notable positive was how quickly Cameron and the other DBAs were able to come up to speed on Hedgehog, *without extensive training*. According to Cameron, “We read the manual, played with it for a while on some test servers, watched an online demo, and then we jumped right in.”

The total time span from the point the University first began discussing security improvements until the first copies of Hedgehog were installed, was about 9 months. From there things progressed rapidly, in large part due to Hedgehog’s ease of implementation. Cameron recalls: “Hedgehog was just incredibly easy to deploy. I think it was about a half-hour to install the server – I’ve forgotten because it was such an insignificant amount of time. And then each sensor took about 5 minutes to install, so that’s been brilliant as well, really.”

Results, Benefits and Future Plans

The team at University of Bristol could not be happier with the initial results of its real-time database activity monitoring and virtual patching implementation. They not only have full visibility into all suspicious database access via immediate alerts, but on the most sensitive data they termininate unauthorized access in real-time, potentially preventing a costly breach before it can occur.

When asked if there were any surprises, Cameron’s response is quite telling: “Prepare yourselves to be scared by what you see in the alerts. While many of the SQL injection alerts are not necessarily malicious activity – they are often just the result of poor coding practice – they each represent a potential vulnerability that could have easily been exploited before installing Sentrigo.” Mark Ellingsen, Web & Database Team Manager, added, “One of the best things to come out of this project has been the ability to reach out to developers and close these gaps. They were just as shocked as anyone.”

In addition to database activity monitoring, for systems where an application either cannot be certified to work on a patch from the database vendor, or downtime cannot be scheduled for an extended period, database instances are now protected using virtual patches. Any attempts to exploit the unpatched vulnerability will immediate trigger either an alert or a termination, depending on the perceived severity of the threat.

Furthermore, as this was the first major security project on this scale across the University, many of the processes the team put in place are now being used for other projects as well. The learning and leadership is having an influence beyond the database group, raising the overall awareness of security best practices throughout the University.

The first phase focused on those databases and applications with the most sensitive information, and therefore addressed data assets that would be most damaging if they were breached. The team is now actively working to roll out protection for all databases across the University of Bristol. In parallel, the team continues to build out more granular custom rules to provide the highest level of protection for critical data: for example, limiting access to certain tables to only a small number of specified users coming from specific hosts. In the domain of information security it seems like one is never quite done, but with the combination of Sentrigo’s Hedgehog suite and the team at the University of Bristol, data protection is stronger than ever.