MOBILE

ABOUT US REGISTER LOGIN

BIGDATA REPUBLIC | Transform Your Business With Data

HOME BLOGGERS MESSAGES POLLS WEBINARS RESOURCES VIDEOS | STRATEGY ANALYTICS TECHNOLOGY FB TW LI G+ RSS

FINANCIAL SERVICES HEALTHCARE GOVERNMENT EDUCATION RETAIL

UNIFIED DATA

Hackers Want Your Big Data

Robert Plant, Associate Professor, School of Business Administration, University of Miami
2/11/2013

Comment
13 comments

Login
50% 50%

Recently, there have been many high-profile hacking attacks: stolen passwords from Twitter; snoopers at the NY Times looking for sources; Saudi Aramco was forced to scrap 30,000 computers destroyed by a virus; even Zappos had customers' email addresses, phone numbers, and other personal information (shoe sizes!?) stolen.

Hacking is on the rise. It's easy for even beginners to go online, download a hacker's cookbook, and attack targets. In Austria, a student was recently arrested as a suspect in the hacking of 259 companies in just three months. Even the source code to the infamous Suxnet is available online and has the potential for havoc in the wrong hands.

Hacking proprietary corporate data
While weakly protected targets such as corporate webpages are attractive for some hackers, the professional hacker is interested in the proprietary corporate data that can be sold or used for other forms of gain. The "big data" data set provides a tempting target. For example, as reported on ZDNet, Utah's Medicaid system was hacked and the personal details of an estimated 780,000 victims were compromised. In Utah, the intrusion followed a hacker motto "opportunity + lack of preparation = success," in that the Utah Department of Technology Services had recently moved all of the claim files to a new server. Unfortunately, the server password authorization processes had not been configured properly, thus opportunely allowing the hackers access.

Big data sets of intellectual property are also attractive targets. In January 2013, two British hackers were convicted of downloading more than 7,000 music files from Sony Music, allegedly including tracks by Elvis Presley; Britney Spears; and unreleased work from Michael Jackson, whose rights had been bought by Sony for $250 million. The release of this music to a free music site would clearly be hugely damaging financially to the company.

Assess security in your big data system
Companies need to take a fresh look at their security in the deployment of very large heterogeneous distributed "big data" systems. Security should be aligned with the value of the content; the disruption factor, and the hit to the brand equity any disruption may have. This is where it gets tricky.

First, the premise of big data is that for many firms, it is a resource that can be tapped by many users across their organization for unstructured queries and analysis. As such, the system is accessible and high profile, not hidden away. Any attempt to hide them would most likely be futile anyway as hackers are looking for them, and peering through the camouflage.

Second, many big data technologies such as Hadoop were not designed at the outset from a security perspective. While the commonly adopted big data stack is very attractive to organizations through as its efficient, effective and accessible attributes; its security component is usually an afterthought. While the Hadoop environment itself lacks the security controls usually associated with commercial grade database systems, and those that are available need to be carefully and properly configured. It is worth once more remembering that that these systems were designed as open systems not "locked down" industrial security strength solutions.

You need to think beyond analytics
As such, firms experimenting with big data deployments need to not just focus on the analytics and the results the system produces but also the security solutions around it, both from operational and infrastructural perspectives. In light of this, there are three basic recommendations:

- **Engage an expert.** Identify and work with a consulting firm that truly understands big data security issues -- they are very different from traditional database security issues, as are the solutions. For example, encryption, usually a good choice for protecting data from prying eyes, is not easily implementable in big data distributed systems.
- **Beware of the quick fix.** The big data stack is not directly amenable to a "bolt-on" security solution, that's off the shelf; each component that you have chosen for your architecture will need careful consideration both with respect to its own security weaknesses such as APIs as well as those of the overall stack interaction. This requires specialist knowledge (see above recommendation!).
- **Think cloud.** Use the resources and technical skills of your cloud provider to host the solution within their security environment wherever possible. They can set "honey traps," deploy systems

MORE BLOGS FROM ROBERT PLANT

A Review: Big Data in 2013
39 comments
Data scientists, NSA, C-suite buy in... Big data changed a lot in the last 12 months.

What Would Seymour Cray Think of Big Data?
13 comments
How would the tech legend respond to the 4 Vs?

The 360 Degree View of a Customer
56 comments
Big data is helping companies like Netflix see what you really want (and even when you go to sleep).

Lessons for Big Data From President Obama's Healthcare Implementation
24 comments
Three big data lessons for CEOs from HealthCare.gov's bumpy start.

Is Big Data Ruining Sports?
29 comments
From sailing to the NBA -- big data could increase the gap between sporting haves and have-nots (while ruining the magic in the process).

More from Robert Plant

FLASH POLL

All Polls

BDR IN YOUR INBOX

Enter email SUBMIT

FEATURED VIDEO

Big Data Explained: What Is Data Governance? 0

A short video over view of the need for data governance.
Watch This Video

More Video Blogs

FOLLOW US ON TWITTER

to monitor unusual access requests and intruder attacks, as well as use their own "big data" analytics to scan security logs.

The reality is that the security associated with big data is unfortunately lagging the deployment of these systems. According to the Gartner Hype Cycle for Application Security 2012 (as reported in Marketvisio); overall "application security" as a category is still five to 10 years away, and other more focused solutions security issues that could help with big data, such as application-security-as-a-service are two to five years away. That's quite a headstart for the bad guys, so it's worthwhile treading carefully in this space, as the downside can be potentially as bad as the upside is potentially good.

Related posts:

- Getting Big Data Results ASAP
- What Big Data Is Not... at Least Not Yet!
- Stop Wasting Time on Visualization
- How Does Your Big Data Stack Up?

— Robert Plant, *Associate Professor, School of Business Administration, University of Miami*

Email This Print Comment

COMMENTS

Newest First | Oldest First | Threaded View

PAGE 1 / 2 > >>

Login

50% 50%

SharCo, User Rank: Petabyte Pathfinder
2/15/2013 | 3:27:54 AM

Re: secure data strategies
Security is one thing that should be constant in all IT efforts. People really shouldn't get complacent at all when it comes to security, because hackers can and will definitely strike when you least expect it.

Reply | Post Message | Edit/Delete | Messages List | Start a Board

Login

50% 50%

SharCo, User Rank: Petabyte Pathfinder
2/15/2013 | 3:26:31 AM

Re: The bad guys always have a head start.
I agree, Saul. We shouldn't ever let fear hold us back, specially when we're at the threshold of innovation. If they strike, we should strike back, or better yet, cut in front of them so they won't be able to do as much damage as they hope to do.

Hackers are everywhere, but that doesn't mean that the good guys are outnumber or can't match them, or overtake them.

Reply | Post Message | Edit/Delete | Messages List | Start a Board

Login

50% 50%

Saul Sherry, User Rank: Blogger
2/13/2013 | 4:33:38 AM

Re: secure data strategies
@mharden - I've been in loads of cloud webinars over the last 6 months, and that security is something most audience members want to ask about.

Cloud + Big Data (which is in a lot of people's plans) ask even bigger security questions - but I would say the answers lie in the process recommended in making your cloud secure.

Build in security to your plans as soon as you start building plans and scope out your vendor to the Nth degree... make sure you are happy with the security options they offer as well as the functionality.

Reply | Post Message | Edit/Delete | Messages List | Start a Board

Login

50% 50%

mharden, User Rank: Exabyte Executive
2/12/2013 | 11:00:05 PM

secure data strategies
Big data will continue to gain momentum placing even greater emphasis on security to protect these large information repositories. What kind of security software and strategies are typically employed to combat the inherent security weaknesses?

Reply | Post Message | Edit/Delete | Messages List | Start a Board

Login

50% 50%

Saul Sherry, User Rank: Blogger
2/12/2013 | 10:09:29 AM

Re: The bad guys always have a head start.
Aha I've got you @SMkinoshita - so we're talking XBOX/ministry of defence size mess ups.

In that case I would imagine a well thought our PR approach is a huge part of this recovery plan.

Reply | Post Message | Edit/Delete | Messages List | Start a Board

Login

50% 50%

smkinoshita, User Rank: Exabyte Executive
2/12/2013 | 10:07:26 AM

Re: The bad guys always have a head start.
@Saul -- A Big Data disaster recovery plan is significantly different. The typical disaster recovery plan has to do with how to deal with direct damage to the company. The Big Data disaster recovery plan also has to include dealing with direct damage to *everyone in the data*.

Usually when a company has a serious loss of equipment or employees, most of its customers won't sue it. With Big Data, not only is the company impacted by the theft, so are the people whose data was in the company's care. So a Big Data disaster recovery plan has to include a way to contact everyone impacted as quickly as possible, ways to dealing with the resulting fallout, and an announcement of how such losses will be prevented in the future.

Reply | Post Message | Edit/Delete | Messages List | Start a Board

Saul Sherry, User Rank: Blogger
2/12/2013 | 8:45:22 AM

Big Data Republic@BigDataRepublic 15 Apr
AllJoyn: A Common Language For Internet Of Things - Open-source lingua franca aims to let IoT devices and services... ow.ly/2FHbY7
Retweeted by Yakamoto
Expand

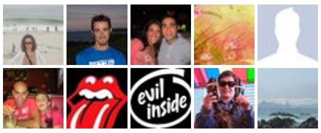
Hajime Ozaki@hajozaki 22h
BDR Top 20 #BigData David Smith David Smith List of top tweeters on Big Data from @BigDataRepublic wp.me/p4Aavi-2
Show Summary

Marcus Borba@marcusborba 28 Apr
#BigData #Analytics #BusinessIntelligence #FS @informationweek @AllAnalytics @BigDataRepublic @BigDataNetwork @BigDataClub

LIKE US ON FACEBOOK

Big Data Republic
Like

4,168 people like Big Data Republic.



Facebook social plugin

ACCOLADES

MEDIA PIONEER AWARDS WINNER 2013

Media Pioneer Award Winner

Login

50% 50%

Re: The bad guys always have a head start.
@netcrawl - this is true - as much as I like to harp on here about how government should be taking advantage of big data, there is always this downside.

Still... we can't let that fear interrupt the great potential... we just need to be smarter and more vigilant.

Reply | Post Message | Edit/Delete | Messages List | Start a Board

Login

50% 50%

Saul Sherry, User Rank: Blogger
2/12/2013 | 8:43:54 AM

Re: The bad guys always have a head start.
Thanks @SMkinoshita - do you see the disaster recovery plan in a big data envirionment differing much from a standard plan? Just bigger?

Reply | Post Message | Edit/Delete | Messages List | Start a Board

Login

50% 50%

Saul Sherry, User Rank: Blogger
2/12/2013 | 8:42:12 AM

Re: The bad guys always have a head start.
@Legalcio - inteteresting that your pragmatic approach here flies in the face of one of the biggest hyped corners of big data so far... To listen to the vendors you would assume the exact opposite... that all members of staff can and should have access to those data stores.

But you are right, there's no need to open it up so wide. Your analysts will be the ones with the insight, and security wise, the smaller the user group the easier to patrol.

Reply | Post Message | Edit/Delete | Messages List | Start a Board

Login

50% 50%

netcrawl, User Rank: Petabyte Pathfinder
2/12/2013 | 3:01:13 AM

Re: The bad guys always have a head start.
I agree! these hackers are always ahead start, they're smart and much sophisticated. As the world of computing evolves, hackers also evolves, adapting to the fast-changing environment. They know that the big data is the future of the information economy.

Reply | Post Message | Edit/Delete | Messages List | Start a Board

PAGE 1 / 2 > >>

BIG DATA REPUBLIC

ABOUT US | CONTACT US | HELP | REGISTER
TWITTER | FACEBOOK | LINKED IN | GOOGLE+ | RSS

in partnership with InformationWeek UBM Tech

powered by UBM DEUSM

bigdatarepublic : /bigdatarepublic/section/2635 : /bigdatarepublic/section/2635/258734

UBM Tech

UBM TECH

OUR MARKETS: **Business Technology** | **Electronics** | **Game & App Development**

Working With Us: Advertising Contacts | Event Calendar | Tech Marketing Solutions | Corporate Site | Contact Us / Feedback