the Availability Digest™

--- achieving 100% uptime

Volume 10
Issue 3

March 2015

The digest of current topics on Continuous Availability. More than Business Continuity Planning.

BCP tells you how to *recover* from the effects of downtime.
CA tells you how to *avoid* the effects of downtime.

www.availabilitydigest.com

Follow us
@availabilitydig

Thanks to This Month's Availability Digest Sponsor

In this issue:

Browse through our useful links.

See our article archive for complete articles.

Sign up for your free subscription.

Visit our Continuous Availability Forum.

Check out our seminars.

Check out our technical writing services.

Check out our consulting services.

Encryption – A Nuisance or a Necessity?

Will the theft of sensitive information from corporate databases ever stop? It seems that every week we hear of another massive breach in which personal data of millions of people are stolen. During the 2013 holiday season, Target lost 110 million records of card transactions. Early the following year, attackers surreptitiously swiped the account information of 58 million unsuspecting Home Depot customers. In August of last year, the personal information of 4.5 million patients of Community Health Systems was stolen. Early this year, Anthem Blue Cross Blue Shield unwittingly presented information on almost 80 million of its members to hackers.

No matter how smart we are at building extensive security into our systems, it seems that the hackers are always smarter. The only way to stop this theft is to make the information useless to the hackers. This can be accomplished by encrypting all sensitive data in-place.

True, encryption may be an expensive task. But with today's technology in tokenization and format-preserving encryption, it is a manageable task. The cost of encrypting sensitive data must be weighed against the cost of stolen personal information and the inevitable negative publicity. We are increasingly asked in our consulting services and seminars to include security as an aspect of system availability.

Dr. Bill Highleyman, Managing Editor

Never Again

Anthem Loses 80 Million Records to Hackers

Anthem, Inc. is the second largest health insurer in the United States. Part of the Blue Cross Blue Shield (BCBS) health insurance network, Anthem has millions of customers in fourteen states.

On Wednesday, February 4, 2015, Anthem announced that hackers had breached its IT systems and had stolen the personal information of up to 78.8 million BCBS customers and employees. This was the largest data breach to-date of any U.S. health insurer.

The discovery was made by an Anthem database administrator on January 27th. He uncovered a database query running under his login information, a query that he had not initiated. He stopped the query and alerted Anthem's Information Security department. Anthem immediately notified the FBI (the U.S. Federal Bureau of Investigation). Anthem personnel determined that the hack had compromised the logon credentials of five other database administrators and had been in progress for six weeks.

What is unfortunate is that none of Anthem's sensitive database was encrypted in-place. Hacking attacks are going to stop only when corporations make the investment to incorporate encryption into their systems so that stolen information has no value to a hacker. True, this can be a costly move. However, its cost must be compared to the cost and publicity that accompanies a major hack such as the Anthem attack.

--more--

Happy Valentine's Day - But No Flowers

It was a sad Valentine's Day for many in the U.K. this year. The financial-transaction network of Global Payments, Inc., one of the country's largest card-processing firms, suffered an outage on the afternoon of Friday the 13th, leaving shops, restaurants, and bars unable to accept chip-and-pin card payments. The outage lasted for 30 hours until Saturday evening, Valentine's Day. Global Payments blamed the outage on a terminal network service provider.

Diners were turned away from restaurants unless they could pay in cash. Husbands couldn't buy their wives chocolates for Valentine's Day nor order flowers for them over the phone. This was one of the busiest weekends of the year. Many merchants reported revenue losses in the order of tens of thousands of pounds.

Service was finally restored at about 6:30 PM on Saturday afternoon, too late for the Valentine's Day rush.

--more--

Never Again

Facebook Suffers Self-Inflicted Outage

On Tuesday morning, January 27, 2015, at 6:10 AM GMT (10:10 PM PST), Facebook went down for almost an hour. The outage also took down its photo-sharing site, Instagram. The outage affected 1.35 billion Facebook users and 300 million Instagram users worldwide.

The Facebook outage was effectively global, impacting users in the U.S., the U.K., Europe, Asia, Australia, and New Zealand. This was its worst outage in four years.

During the outage, some visitors were greeted with the message, “Sorry, something went wrong.” For others, the Facebook page simply would not load. During the hour-long outage, humans around the globe were forced to interact with each other in person.

It is amazing how much social media has taken over our lives. However, as important as Facebook may be to the well-being of many of us, it is only fair to point out that according to downtime statistics, Facebook has achieved an availability in excess of four 9s for most of the eleven years of its existence. This is an admirable record for a major web site.

--more--

Product Reviews

Stratus Continues its $50,000 Uptime Guarantee

In 2010, Stratus Technologies bet $50,000 that its fault-tolerant ftServer would not go down in the first six months of operation. If you bought a system by the end of February, 2010, and if it failed in its first six months of operation, Stratus would pay you $50,000 in cash (or in product credit if you preferred).

How did it do on this wager? It performed so well that Stratus announced several extensions to the guarantee. Five years later, it is sticking to its promise. During this entire time, Stratus has not paid out a cent, thus illustrating its claim that ftServers achieve over five 9s of availability.

Stratus’ fault-tolerant systems change the focus of availability from hardware failures and operating-system faults to other factors. Application bugs, operator errors, and environmental faults such as power, cooling, and data-center destruction now become the things about which to worry most.

Continuous availability is no longer a technological problem. It is an exercise in balancing system cost with downtime cost. Stratus’ ftServer is an affordable starting point to achieve extreme availabilities. Stratus says so – with its wallet.

--more--

Tweets

@availabilitydig – The Twitter Feed of Outages

A challenge every issue for the Availability Digest is to determine which of the many availability topics out there win coveted status as Digest articles. We always regret not focusing our attention on the topics we bypass.

Now with our Twitter presence, we don't have to feel guilty. This article highlights some of the @availabilitydig tweets that made headlines in recent days.

--more--

Sign up for your free subscription at http://www.availabilitydigest.com/signups.htm

Would You Like to Sign Up for the Free Digest by Fax?

Simply print out the following form, fill it in, and fax it to:
Availability Digest
+1 908 459 5543

Name: _____

Email Address: _____

Company: _____

Title: _____

Telephone No.: _____

Address: _____

_____

_____

The Availability Digest is published monthly. It may be distributed freely. Please pass it on to an associate.
Managing Editor - Dr. Bill Highleyman editor@availabilitydigest.com.