the Availability Digest™
--- achieving 100% uptime
Volume 10
Issue 8
August 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

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.

Will the "Internet of Things" Be Secure?

Probably not! The "Internet of Things" (IoT) is upon us now. True, it is starting out at the high end. In airliners, avionics instruments and controls are interconnected by an Intranet, as are the cabin facilities. The same technology is used in automobiles. The fifty-some-odd computers in a new car are Intranet-connected, as are the entertainment and climate control systems.

However, security already is being compromised. The avionics and cabin-control systems in airplanes are separated by a firewall, as are the computer systems and the passenger facilities in cars. However, researchers have already shown that an airliner or automobile can be taken over by a hacker (see "Can An Airliner Be Hacked" in our May 2015 issue and "My Jeep Wasn't Hacked!" in this issue).

Estimates predict that there will be five billion IoT devices by the end of this decade. When it comes to smart toasters and light bulbs connected to your home Intranet, it is fruitless to expect that the manufacturers will have invested in the cost of additional memory to provide security. These devices will be hackable. Your toaster, for instance, might suddenly shut off the water to your house.

We at the Availability Digest have now added the impact of security challenges to its seminars and articles on high- and continuous availability. Give us a call to discuss our services.

Dr. Bill Highleyman, Managing Editor

Never Again

Ashley Madison Cheats Exposed

Ashley Madison is the premiere website for the married who wanted to cheat on their spouses. Ashley Madison's slogan is "Life is short. Have an affair." The worst has happened for members of the web site. Its database has been hacked and has been posted online for all to see. With a quick search of an email address, spouses can find out if their "better" halves have been trying to cheat on them.

The 60 gigabyte database exposing 37 million members has been posted on the Dark Web and is accessible only to those with a Dark Web browser. Several sites that republished the data on the public Internet have been closed down for copyright reasons. However, one web site has survived. It will accept an email address and will indicate whether or not the address is in the database.

The Ashley Madison hack should be a reminder to all that the Internet is public and perpetual. Whatever you do on the Internet is likely to remain accessible for years to come, whether it's a membership in a secret society or a posting on a Facebook page.

--more--

Do the Russians Have Your Tax Returns?

In August, 2015, the U.S. Internal Revenue Service (IRS) announced that one of its systems had been breached and that the tax returns of over 334,000 taxpayers had been stolen. Already, tax returns for $50,000,000 in fraudulent tax refunds have been filed.

In this attack, the cybercriminals did not secrete malware on the IRS system to give them a back door for access. Rather, they logged on as legitimate taxpayers. Using social media such as Facebook, they acquired vast amounts of data about taxpayers, which allowed the cybercriminals to begin the logon procedure. The attackers also had to determine (or guess) the answer to several personal security questions.

This data breach is concerning because the IRS system was not hacked. Rather, a very sophisticated approach was taken. A massive amount of data was acquired on each of the taxpayers from non-IRS sources and was used to log on to the system as the taxpayers themselves. In effect, the hackers came in through the front door. Any system, no matter the amount invested to make it secure, is subject to this sort of attack.

--more--

Availability Topics

My Jeep Wasn't Hacked!

Jeeps are being hacked! A pair of security researchers has demonstrated remote control of a Jeep by turning on its air conditioner and its radio, activating its windshield wipers, and putting it in neutral while moving. They also can disable the brakes and control the steering and the accelerator. Fortunately, my Jeep is not one of those affected – it is just a couple of years too old.

In a recent *Availability Digest* article, we described a security researcher who was able to access a plane's flight controls via the in-flight entertainment system in the cabin. It turns out that the cabin Intranet network and the flight-control avionics Intranet network were linked by a firewall, and he was able to breach the firewall.

Now this malicious technology has been extended to automobiles. Security researchers have demonstrated that they can take control of a car's computers by accessing it via the car's infotainment (information and entertainment) center using a cell phone even thousands of miles away. The infotainment center's Intranet and the Intranet connecting the car's computers are separated only by a firewall, which they were able to breach.

--more--

Recommended Reading

2015 Verizon Data Breaches Investigation Report

Every year for the last several years, Verizon has performed an extensive survey on data breaches and has published its findings in a detailed Data Breach Investigations Report (DBIR). We summarize their findings for the year 2014 in this article.

The 2015 report includes input from 70 contributing organizations from around the world. Verizon distinguishes between security incidents and data breaches. A security incident is any event that compromises the confidentiality, integrity, or availability of an information asset. A data breach is an incident that results in confirmed disclosure (not just exposure) of data to an unauthorized party. The 2015 report is based on 79,790 security incidents and 2,122 confirmed data breaches.

The data is broken down into 20 different industry categories. The top three industries affected by security incidents are public services, information, and financial services.

The report concludes that 40% of all incidents could have been detected and stopped via simple, critical security controls.

--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.