

Security Challenges of Cloud Computing

Joe St Sauver, Ph.D. (stsauver@fsi.io)

Scientist, Farsight Security, Inc.


161 STEELHEAD
<https://www.stsauver.com/unc/>

University of North Carolina
Fedex Global Education Center
Thursday, October 19th, 2017

Today's Agenda

I.	Introduction	3
II.	Hype and Jargon	8
III.	The Cloud and Security	20
IV.	Is "Cloud" Cyber Security Different Than "Regular" Cyber Security?	26
V.	Cloud Risks: Availability	31
VI.	Cloud Risks: Confidentiality	43
VII.	Cloud Risks: Integrity	53
VIII.	Integrating With The Cloud	64
IX.	Cloud Provider Choice: Go With Cloud Provider Foo, Or Not?	70
X.	Cloud Security Alliance Cloud Controls Matrix (CSA CCM)	79
XI.	Conclusion	88

I. Introduction

"In my mind I'm goin' to Carolina
Can't you see the sunshine?
Can't you just feel the moonshine?
Ain't is just like a friend of mine
To hit me from behind"

James Taylor, *Carolina In My Mind* (1968)

Thanks (And A Disclaimer)

- I'd like to begin by thanking **Mr. Tim Cline**, UNC Information Security Office, for the invitation to talk with you today. It's an honor to be here!
- Thank you, too, to **Mr. Bob Blanchard** for handling logistics, and to the whole Information Technology Team at UNC Chapel Hill.
- I'd also be remiss if I failed to thank my boss at Farsight Security, **Mr. Ben April**, for permission to be with you here today.
- Most importantly, however, I'd like to thank all of **YOU** for making the time to attend and participate in today's program. I know you're all very busy ladies and gentlemen.
- That said, the remarks I'll share today represent solely my own perspective, and do not necessarily represent the opinion of Farsight Security, UNC, or anyone else.

A Little About My Background

- I worked for ~28 years for the **University of Oregon Computing Center** in Eugene, up to and including having responsibility for all academic computing at the University of Oregon.
- Overlapping that time at UO, I was also **Internet2's Nationwide Security Programs Manager** under a UOregon-Internet2 contract. (You may know that Internet2 is higher education high speed network backbone.)
- While working under contract for Internet2, I ran the **InCommon SSL/TLS Certificate Service** and the **InCommon Duo Multifactor Program** for Internet2. I note that UNC subscribes to both of those
- **My responsibilities with Internet2 ALSO included security assessments relating to many potential Net+ cloud offerings.**
- My \$DAYJOB now? Scientist with Paul Vixie's start up company, **Farsight Security, Inc.**

Engagement With The Cyber Security Community

- My cyber-security-related work goes beyond the work I do for Farsight.
- By special permission of the REN-ISAC Board, I remain an XSEC member of the **Research and Education Network Information Sharing and Analysis Center (REN-ISAC)**. I also serve on the REN-ISAC Technical Advisory Group.
- I'm also one of half a dozen senior technical advisors for the **Messaging, Mobile and Malware Anti-Abuse Working Group (M3AAWG)**, working closely with M3AAWG's anti-Pervasive Monitoring SIG and Domain Name Abuse SIG.
- I'm also active in a number of other cyber security activities.
- **Copies of publicly available talks and other materials of mine are available from my website at <https://www.stsauver.com/joe/>**

A Note About The Odd Format Of My Talks

- You may notice that my talks (including this one) are NOT formatted like most other folks' talks. My format is more verbose.
- Sometimes people wonder why...
- Most importantly, unless I'm tightly structured, **I tend to ramble and run over.**
- **I know I cover a lot of material.** You'll need notes. I provide them.
- **If you missed listening to this talk,** these slides should let you figure out what I went over.
- My talk format **works well for indexing by Google/Bing/etc.**
- **I hate being misquoted.** Detailed slides reduce misquotation risk.
- Some audience members may be **deaf (or hard of hearing).** These notes are meant to help make this content accessible for them.
- I won't just read these slides word-for-word to you, and you shouldn't try to do so in real time, either.

II. Jargon

"Biggie Biggie Biggie can't you see
Sometimes your words just hypnotize me
And I just love your flashy ways
Guess that's why they broke, and you're so paid"

The Notorious B.I.G., *Hypnotize* (2014)

Some Cautions About "The Cloud"

- As you likely already know, there's a **LOT of hype** associated with "cloud computing."
- Cloud computing is a huge topic, encompassing diverse models and technologies, even though users and the trade press tend to lump them under a common name. Covering it all in an hour for a general audience is simply impossible.
- Cloud computing is still a work-in-progress. Because it is rapidly evolving, what I tell today you may quickly become irrelevant or obsolete.
- Nonetheless, there's so much thrust behind cloud computing that **we simply don't have the option of sitting back and waiting.**

"So What Is The Cloud?" Three Provider Definitions

- "'Cloud computing' (also called simply, 'the cloud') describes the act of storing, managing and processing data **online** — as opposed to on your own physical computer or network." *[nonspecific (JS)]*
<https://www.rackspace.com/en-us/cloud/cloud-computing>
- "[...] cloud computing is the delivery of computing services —servers, storage, databases, networking, software, analytics, and more — **over the Internet (“the cloud”)**. Companies offering these computing services are called cloud providers and typically charge for cloud computing services based on usage [...]" *["the Internet" should not taken as synonymous with "the cloud" (JS)]* <https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/>
- "Cloud computing is the on-demand delivery of compute power, database storage, applications, and other IT resources through a **cloud services platform via the internet** with pay-as-you-go pricing." <https://aws.amazon.com/what-is-cloud-computing/>
[nice recursive def'n, cloud defined as "cloud services platform" (JS)]
- See also <https://csrc.nist.gov/publications/detail/sp/800-145/final>

Generally Accepted Characteristics

- Most people would agree that true cloud computing...
 - Usually has low (if not zero) up front capital costs for its users.
 - It largely eliminates operational responsibilities (e.g., if a disk fails or a switch loses connectivity, you don't need to fix it)
 - For the most part, cloud computing eliminates specific knowledge of WHERE one's computational work is being done; (although you MAY know a general "region" where it happens)
 - Offers substantial elasticity and scalability: if you initially need one CPU, that's fine, but if you suddenly need 999 more, you can get them, too (and usually with very little delay!). If/when demand drops, you can scale your usage back, too.
 - Cloud computing leverages economies of scale (running mega data centers with tens of thousands of computers is far less expensive (per computer) than running a small cluster)
 - Is normally pay-for-what-you-use, often by credit card.

Some "Clouds" Won't Necessarily Have All of Those Characteristics

- For instance, if your site is running it's own **LOCAL** private cloud:
 - There WILL be capital expenditures up front,
 - You (or someone at your site) WILL still care about things like hardware failures,
 - You likely WON'T have the illusion of a seemingly infinite inventory of processors (or memory or disk), and
 - You may not pay *ala carte*

Nonetheless, a local private cloud service may functionally work the same way as a public cloud service, and hybrid cloud models may even combine private and public cloud services in a fairly seamless way. The underpinnings are often the same (e.g., see for example <https://www.ubuntu.com/cloud>)

The Three Main Types of Cloud Computing

- **Infrastructure as a service (IAAS)** (raw capacity from Amazon, Microsoft Azure, etc.). Limited number of major providers with at-scale offerings. (Think "system admins")
- **Platform as a service (PAAS)** (less common/less popular, see [https://www.skyhighnetworks.com/cloud-security-blog/microsoft-azure-closes-iaas-adoption-gap-with-amazon-aws/for \\$ graphs](https://www.skyhighnetworks.com/cloud-security-blog/microsoft-azure-closes-iaas-adoption-gap-with-amazon-aws/for%20graphs)). Typified by <https://cloud.google.com/appengine/> or <https://www.openshift.com/> (Think "focused on enabling developers to be more efficient")
- **Software as a service (SAAS)** (Gmail, Box, Salesforce, various online desktop backup solutions, etc.). Very common/very diverse/very well-known by the general public. (Think "end users")
- Let's dig into the first and the third of those a little...

Infrastructure As A Service

- IAAS differs from traditional "virtual hosting" in that shared capacity can easily be provisioned dynamically with "low friction;" grow or contract your infrastructure as required. This is great for businesses with irregular/"spikey" load patterns.
- On the other hand, you WILL "pay for what you eat" (rather than paying a flat rate per month for dedicated capacity).
- By implication, **your revenue had better scale up with your usage**, or you'll be potentially looking at a BIG bill with no cash to pay it (pricing is publicly available for Amazon's cloud services at <https://aws.amazon.com/ec2/pricing/> if you want to take a look)
- Cloud IAAS is **heavily network reliant**.
- **IAAS is seductive**: Suddenly, hardware's not your problem. IP address space is not your problem. Physical space in the colo is not your problem. Power and cooling are not your problem, etc.

In Contrast, Software As A Service (SAAS)...

- The easiest way to explain SAAS is by pointing to some example services...
- Hosted email, video conferencing, messaging
- Online backup services and file sharing services
- Backend business processing (such as expense reporting), etc.
- **This niche can have huge players (like Google or Microsoft), but it can also have services fielded by a couple of programmers working out of their garage, and everything in-between.**
- **WHATEVER form it takes, we know "the cloud" is a major trend...**

It Seems As If EVERYONE's Now At Least Considering the Cloud

- **"94% of Enterprises are at least discussing cloud or cloud services"**

"Avoiding the Hidden Costs of the Cloud," PDF page 4,
<http://www.symantec.com/content/en/us/about/media/pdfs/b-state-of-cloud-global-results-2013.en-us.pdf>

[There are a MILLION stats/surveys/reports about all things cloud, as you'll quickly see]

What's Driving That Interest in Cloud Computing?

- Thought leaders: Amazon, Google, Microsoft and many other Internet thought leaders have all aligned behind "the cloud"
- Mobile devices: Smart phones, tablets and Chromebooks typically have limited on-device storage and processing power may also be limited due to intentional use of energy-efficient ARM processors. The cloud is a perfect compliment to those mobile devices, offering virtually unlimited storage and infinite processing power.
- Costs: Because cloud computing should theoretically help sites avoid major new **capital expenditures** (capex) while also controlling some ongoing operational expenses (opex), cloud computing is potentially a lifesaver for financially strapped businesses, including many universities. **"It's cost effective."**

But Is The Cloud Cost Effective? It Depends...

- Consider the report "***Why Switching to AWS May Cost You A Fortune***" by HiVelocity, which states:

Every month we lose a couple of customers to Amazon's Cloud or AWS (Amazon Web Services) and every month we have another couple of customers sign up with us having just cancelled their AWS solution. Each time their reasoning for leaving AWS is the same, "way more expensive and way less performance than we expected, especially when compared to what we get from a dedicated server".

See <https://www.hivelocity.net/blog/AWS-bandwidth-expensive>

[not to ruin the surprise, but the issue is often cloud bandwidth charges]

Ultimately, Sites Either Use Cloud Services Or They Don't

- Whatever the reason, we know that **only "about 28% of North American and European enterprise infrastructure technology decision-makers indicate that their firms have adopted public cloud."** <https://go.forrester.com/wp-content/uploads/Predictions-2017-Customer-Obsessed-Enterprises-Launch-Clouds-Second-Decade.pdf> at page 2.
- **Many times the biggest hurdle is security.**

III. The Cloud and Security

"[...] reminds me of a warm safe place
Where as a child I'd hide
And pray for the thunder
And the rain
To quietly pass me by [...]"

Guns N' Roses, *Sweet Child O' Mine* (1987)

Security Remains A Major Barrier To Cloud Adoption

- **"Study Reveals Biggest Barrier to Cloud Adoption:**

"The survey from HyTrust, called the State of the Cloud and Software-Defined Data Center (SDDC) 2016, was given to 500 C-level and vice president executives who lead medium- and large-sized organizations, mostly in the private sector [* * *]

"The study found that the perennial concern executives have with cloud adoption is security. About 67 percent said security concerns will slow cloud migration, while 55 percent predicted more data breaches and security problems."

<http://www.govtech.com/computing/Study-Reveals-Biggest-Barrier-to-Cloud-Adoption.html> (April 26, 2016)

What Gets Moved Into The Cloud May Not Stay There. Why? Again, "Security Concerns"...

- "IDG Enterprise recently published Cloud Computing: Key Trends and Future Effects Report, showing how enterprises continue to struggle with security, integration and governance [...] IDG's methodology is based on interviews with 1,358 respondents [...] **42% of cloud-based projects are eventually brought back in-house, with security concerns (65%),** technical/oversight problems (64%), and the need for standardization (on one platform) (48%) being the top three reasons why. [...] **For IT, concerns regarding security (66%),** integration stability and reliability (47%) and ability of cloud computing solutions to meet enterprise/industry standards (35%) **challenge adoption.**
- <http://www.forbes.com/sites/louiscolumbus/2013/08/13/idg-cloud-computing-survey-security-integration-challenge-growth/>

Other Times, PLANS to Move-To-The-Cloud May End Up UNREALIZED—The NASA Example

- The 2013 NASA OIG Report: 'Over the past year [e.g., 2012] NASA spent **less than 1 percent of its \$1.5 billion annual IT budget on cloud computing**. However, moving forward, the agency plans to dedicate much more to cloud security and initiatives. **Within the next five years, NASA is planning to have up to 75 percent of its new IT programs begin in the cloud and 100 percent of the agency's public data stored in cloud.**'

"NASA Falls Short on Its Cloud Computing Security," http://news.cnet.com/8301-1009_3-57596053-83/nasa-falls-short-on-its-cloud-computing-security/ [emphasis added]

- The 2017 NASA OIG Report: "[NASA has] moved **just over 1 percent of eligible Agency data into approved cloud services.**"

"Security Of Nasa's Cloud Computing Services," <https://oig.nasa.gov/audits/reports/FY17/IG-17-010.pdf> [emphasis added]

Cloud Provider Facility Locations

- You may want to know where your cloud lives.
- For example, one of the ways that cloud computing companies keep their costs low is by locating their mega data centers in locations where labor, electricity and real estate costs are low, and network connectivity is good.
- Thus, your cloud provider could be working someplace you may never have heard of (such as The Dalles, Oregon, or Lenoir, NC) where power is cheap and fiber is plentiful – or even **overseas**.
- If your application and data do end up at an international site, those systems will be subject to the laws and policies of that jurisdiction. Are you comfortable with that framework?
- Are you also confident that transoceanic connectivity will remain up and uncongested? Can you live with the latencies involved?
- And what about physical security of these billion dollar sites?

If You ARE Mainly Worried About Physical Security

- ... this is the **wrong talk**. I've got a **different talk** about physical security. See "Physical Security of Advanced Network and Systems Infrastructure" from April 2011 at <https://www.stsauver.com/joe/phys-sec-i2mm/phys-sec-i2mm.pdf> (89 slides)
- Today, however, we're going to focus on the **non-physical** security exposures associated with "the cloud."

IV. Is "Cloud" Cyber Security Different Than "Regular" Cyber Security?

"Well he's tellin' us this
And he's tellin' us that
Changes it every day
Says it doesn't matter"

Joe Walsh, *Rocky Mountain Way* (1973)

In Many Ways, "Cloud Computing Security" Is The SAME AS Than "Regular Security"

- **Weak passwords are the same**, whether used with a regular server or a server hosted in the cloud.
- As another example, many applications interface with end users via the web. **All the normal OWASP web security vulnerabilities** -- things like SQL injection, cross site scripting, cross site request forgeries, etc. -- are just as relevant to applications running in the cloud as they are to applications running on local conventional servers or servers at a hosted datacenter.

Cloud Computing and Virtualization

- Similarly, cloud computing is built on top of virtualization. Thus, if there are security issues with virtualization, then there will also security issues with cloud computing's use of virtualization.
- For example, could someone escape from a cloud virtual machine instance to the cloud server's host OS? Well, virtual machines **have** experienced issues with jail breaks... For example: "**Xen Patches 'Worst'-Ever Virtual Machine Escape Vulnerability: Bug remained undetected for seven years and enabled complete control of host system.**" <https://www.darkreading.com/endpoint/xen-patches-worst-ever-virtual-machine-escape-vulnerability/d/d-id/1322925?> (10/30/2015): "[...] In an advisory issued yesterday, the Xen Project described the now patched vulnerability as one that could allow the administrator of a guest VM to escalate privileges and take complete control of the host system."

Cloud Computing And Firewalls

- I'm not a huge fan of firewalls (as I've previously discussed in "Cyberinfrastructure Architectures, Security and Advanced Applications," see <https://www.stsauver.com/joe/architectures/architecture.pdf>), but some sites do find value in sheltering at least some parts of their infrastructure behind a firewall.
- Cloud providers can support that approach. For example, see "Amazon Web Services: Overview of Security Processes" whitepaper linked from <https://aws.amazon.com/whitepapers/overview-of-security-processes/> which states:
Firewall: Amazon EC2 provides a complete firewall solution; this mandatory inbound firewall is configured in a default deny-all mode and Amazon EC2 customers must explicitly open the ports needed to allow inbound traffic. The traffic may be restricted by protocol, by service port, as well as by source IP address (individual IP or Classless Inter-Domain Routing (CIDR) block).

In Other Ways, The Cloud IS VERY Different...

- In the cloud, customers normally can't directly assess hardware-level operating system installations, or admin network devices or shared security systems; we need to trust the expertise of the cloud provider's team, instead
- Security capex/opex is fixed and bundled in as part of the service; my choice is effectively "do it" or "don't do it" (or nag/pick at the provider in an effort to potentially get them to make changes). Most services do not offers "tiers" of security.
- That said, what are the general categories of issues/risks we seem to be facing in the cloud?

V. Cloud Risks: Availability

"I'll be there for you
When the rain starts to pour
I'll be there for you
Like I've been there before
I'll be there for you"

The Rembrandts, *I'll Be There For You* (1995)
(opening song from the popular TV comedy series *Friends*)

The "A" in The Security "C-I-A" Objectives

- There are three general security objectives:
 - Confidentiality
 - Integrity
 - Availability
- **Availability is the area where cloud based infrastructure appears to have had its largest (or at least most highly publicized) challenges to date.**
- For example, consider some of the cloud-related outages which have been widely reported...

Major Cloud Outages in 2017 (as of August 1st)

- Nice summary in "**The 10 Biggest Cloud Outages of 2017 (So Far)**"
<http://www.crn.com/slide-shows/cloud/300089786/the-10-biggest-cloud-outages-of-2017-so-far.htm>
- A couple of examples...
- "**AWS, February 28: This was the outage that shook the industry.** An Amazon Web Services engineer trying to debug an S3 storage system in the provider's Virginia data center **accidentally typed a command incorrectly**, and much of the Internet – including many enterprise platforms like Slack, Quora and Trello – was **down for four hours**. [...]"
- "**Microsoft Azure, March 16:** Storage availability issues plagued Microsoft's Azure public cloud for more than **eight hours**, mostly affecting customers in the Eastern U.S. [...] A Microsoft engineering team later identified the culprit as a storage cluster that **lost power** and became unavailable."

Dyn, DDoS'd Off The Air

Dyn DDoS attack exposes soft underbelly of the cloud

The DDoS attack against Dyn affected numerous websites, but the biggest victims are the enterprises that rely on SaaS for critical business operations

It's apparently possible that a DDoS attack can be big enough to break the internet -- or, as shown in the attack against ISP Dyn, at least break large parts of it.

The DDoS attack against Dyn that began Friday went far past taking down Dyn's servers. Beyond the big-name outages, organizations could not access important corporate applications or perform critical business operations.


See: <https://www.infoworld.com/article/3134023/security/dyn-ddos-attack-exposes-soft-underbelly-of-the-cloud.html>

It's Not Just The Network or the DNS: Storage Can Be Key, Too

Cisco loses customer data in Meraki cloud muckup

'Erroneous policy' upload deleted custom apps, IVR menus and custom bling

By [Simon Sharwood](#), APAC Editor 6 Aug 2017 at 23:19

22 

Cisco has admitted to a cloud configuration cockup that erased customer data.

The networking giant [explained](#): “On August 3rd, 2017, our engineering team made a configuration change that applied an erroneous policy to our North American object storage service and caused certain data uploaded prior to 11:20AM Pacific time on August 3 to be deleted.”

“Our engineering team is working over the weekend to investigate what data we can recover,” Cisco's advisory says, adding that the company is working on “tools we can build to help our customers specifically identify what has been lost from their organization.”

Source: https://www.theregister.co.uk/2017/08/06/cisco_meraki_data_loss/

Power Issues Continue To Be A Challenge For Enterprise Data Centers As Well As "The Cloud"

Delta Data Center Outage Grounds Hundreds of Flights

Airline attributes outage to power problem in Atlanta data center

Yevgeniy Sverdlik | Aug 08, 2016

Delta Airlines hasn't yet explained the outage in Atlanta this morning, which led to the grounding of hundreds of flights the day.

It said a power outage "impacted Delta's operations" but a spokesman for the utility who spoke to **Wall Street Journal** that there were no problems on Monday. The utility, Georgia Power, is helping Delta fix a problem with switches.



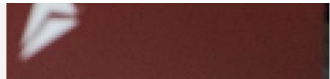
Ed Bastian, CEO, Delta Air Lines, in a video apologizing to customers for disruption of travel caused by a data center outage in August 2016 (Source: Delta)

Delta: Data Center Outage Cost Us \$150M

Price tag extraordinarily high in comparison to data center industry average

Yevgeniy Sverdlik | Sep 08, 2016

The Delta Airlines data center outage that grounded about 2,000 flights over the span of three days in August cost the company \$150 million, the airline's representatives told the audience of a transportation industry conference in Boston Wednesday.



Travelers wait in line at the Delta check-in counter at LaGuardia Airport, August 8, 2016 in the Queens borough of New York City. Delta flights around the globe were grounded and delayed on Monday morning due to a system outage. (Photo by Drew Angerer/Getty Images)

<http://www.datacenterknowledge.com/archives/2016/09/08/delta-data-center-outage-cost-us-150m>

Mitigating Cloud Computing Availability Issues

- Risk analysts will tell you that when you confront a risk, you can try to eliminate the risk, you can mitigate/minimize **the impact** of the risk, or you can simply accept the risk.
- If you truly require non-stop availability, the normal solution is to add redundancy. It's unlikely that all sites you're using will all be down the same time
- To help with that, some cloud computing services offer service divided into multiple "regions." By deploying infrastructure in multiple regions, isolation from "single-region-only" events (such as the power outage mentioned previously) can be obtained.
- Sometimes, though, it may simply make financial sense for you to just accept the risk of a rare/brief outage. Remember:
99.99 availability==> less than an hour of downtime/year;
99.9 availability==> less than 9 hours of downtime/year)
- ***Are you really willing to double your costs to cover 9 hours down?***

How Do We Know That We're Appropriately "Managing" Risk (Assuming We Are)

- *Professional Expertise* ("I'm not *detecting* us getting hit, and I'm not *hearing reports* that we've been hit, and I've managed all the security risks I've been able to, so...")
- *Historical Reputation*: we haven't been hacked previously, so we must be okay ("prior performance doesn't guarantee future...")
- *Expenditures*: we're spending everything we've been able to get for securing things (but what if you've got a security person who's bad at playing organizational "budget war games"?)
- *Audit*: the auditor doesn't return any findings (but what if we've got a crumby auditor who isn't paying attention?)
- *Common Sense Test*: if something bad happens, will what we're currently doing pass the public "sniff test"? That is, are we doing what a reasonable person would normally do?
- **Remember: not everything is "mission critical."**

"Facebook DOWN: Social network NOT WORKING after massive web and app outage" (Oct 11, 2017)

[* *] Users have [...] flocked to Facebook's big rival Twitter to report issues with the service this afternoon.*

One user tweeted: "FACEBOOK IS DOWN"

While another said: "OMG! Facebook is DOWN! What do we do? It's a crisis."

And one fan even suggested it was the end of the world saying: "What happened to Facebook!? It's actually DOWN. The apocalypse must be here!! #facebookdown."

<http://www.express.co.uk/life-style/science-technology/865161/Facebook-DOWN-not-working-outage-why-log-in>

The Ultimate Availability Problem: Bankruptcies

blogs.wsj.com/venturecapital/2013/10/01/nirvanix-files-for-chapter-11-bankruptcy/

October 1, 2013, 6:11 PM

Nirvanix Files for Chapter 11 Bankruptcy

Article

Comments (4)

Email

Print

f

t

g+

in

A

A

By [DEBORAH GAGE](#) [CONNECT](#)

Cloud storage company [Nirvanix Inc.](#) on Tuesday filed for Chapter 11 bankruptcy in Delaware federal court, the culmination of a startling flop for what was once seen as a high-flier among cloud startups.

The filing comes on the heels of a notice the company posted on its website last week saying that it was working with International Business Machines Corp. to either return customers' data or help them move it to another cloud storage provider and would try to be available through October 15.



Kharisma Tarigan/Agence France-Presse/Getty Images

Nirvanix had raised more than \$70 million in venture capital since its founding in 2007, according to VentureWire records. In May 2012 after the last funding round, which was \$25 million, [former Chief Executive Scott Genereux told VentureWire](#) that Nirvanix was growing and headed toward profitability and a possible IPO.

Its largest equity holders are [Khosla Ventures](#) and [TriplePoint Capital](#), which may

Cloud Bankruptcy Concerns...

- If you prepaid (to lock in prices/get a multiyear discount), is that prepaid money safely in escrow somewhere (and able to be refunded), or is it flat out **gone**?
- Can you find a replacement provider that will be able to take over when it comes to providing the same service that your former cloud provider delivered? (standardized services offered by multiple providers will obviously be easier to replace than unique or bespoke applications)
- If there were custom modifications made to the software you were using, do you have copies of what was changed, and could you replicate them elsewhere?
- Perhaps most critically: can you get your data out, and in format that's usable elsewhere? (Proprietary formats should make the hair on the back of your neck stand up.)

Cloud Lock-In: If You Want To Exit The Cloud, Will You Still Have the Required Local Expertise?

- A risk of letting someone else do the "heavy lifting" for you: if you ever need to resume doing that work yourself, it can be a lot harder to "get your strength back" than you might think:
- Will you still have key staff?
- Will you still have critical equipment and facilities?
- Can you deliver the professional quality of the services or application you got from the cloud? (you might not think I think so, but actually, some parts of the cloud work pretty dang well)
- Or is this a case of "Welcome to Hotel California:" you can check out, but you can never leave?

VI. Cloud Risks: Confidentiality

"I'm gonna give all my secrets away
All my secrets away, all my secrets away"

One Republic, *Secrets* (2009)

Data Confidentiality and Breaches

- Let's not get rat holed on availability. It's a big issue, but not the only one.
- Executives and IT leaders don't get fired for services going down (at least as long as they don't go down for TOO long). IT people do get fired when big data breaches involving PII occur. (see the following slide)
- Therefore, most executives and IT people worry a lot about the security of private data, including its security if stored off-site.
- Should they? Yes. Recent breaches in cloud SAAS offerings illustrate the scale of the problem.

"How to get fired in 2017: Have a security breach"

OFFENSE	PERCENT OF COMPANIES WHERE THIS IS A FIREABLE OFFENSE
Failure to meet regulatory compliance that led to large fine or other penalty	68%
Tech investment that leads to a security breach	39%
Data breach that does become public	38%
Failure to modernize your organization's security program	33%
Data breach whose cause cannot be determined	21%
Data breach that does not become public	17%
Failure to meet project deadlines	15%
Authorizing tech investments that are demonstrated not to scale to meet tomorrow's demands	13%
Security product/program investment that fails	13%
Other	3%

Source: <https://www.csoononline.com/article/3158825/it-jobs/how-to-get-fired-in-2017-have-a-security-breach.html>

Example Breach: 198 Million Voter Records Exposed

In what is the largest known data exposure of its kind, UpGuard's Cyber Risk Team can now confirm that a misconfigured database containing the sensitive personal details of over 198 million American voters was left exposed to the internet by a firm working on behalf of the Republican National Committee (RNC) in their efforts to elect Donald Trump. The data, which was stored in a publicly accessible cloud server owned by Republican data firm **Deep Root Analytics**, included 1.1 terabytes of entirely unsecured personal information compiled by DRA and at least two other Republican contractors, **TargetPoint Consulting, Inc.** and **Data Trust**. In total, the personal information of potentially near **all of America's 200 million registered voters** was exposed, including names, dates of birth, home addresses, phone numbers, and voter registration details, as well as data described as "modeled" voter ethnicities and religions.

<https://www.upguard.com/breaches/the-rnc-files>

Yahoo: Three BILLION Accounts Hacked...

#BUSINESS NEWS OCTOBER 3, 2017 / 1:57 PM / 9 DAYS AGO

Yahoo says all three billion accounts hacked in 2013 data theft

Jonathan Stempel, Jim Finkle

5 MIN READ

(Reuters) - Yahoo on Tuesday said that all 3 billion of its accounts were hacked in a 2013 data theft, tripling its earlier estimate of the size of the largest breach in history, in a disclosure that attorneys said sharply increased the legal exposure of its new owner, Verizon Communications Inc ([VZ.N](#)).

<https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82O1>

Protecting Web Data Confidentiality in Transit

- Protecting data in the cloud is often largely a matter of how you encrypt private data at rest, and how you encrypt it when it is in transit/on the wire.
- For web based applications, encryption of data on the wire normally involves use of SSL/TLS ("https"). While all SSL/TLS web sites may look the same, **the quality of the encryption used by any given web site may vary dramatically.**
- **I'd encourage you to check the SSL/TLS practices of cloud (or local) sites you use or rely on using the Qualys SSL/TLS tester that's at <https://www.ssllabs.com/ssltest/>**

Qualys SSL/TLS Report For A Sample UNC Site...



[Home](#) [Projects](#) [Qualys.com](#) [Contact](#)

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > connectcarolina.unc.edu

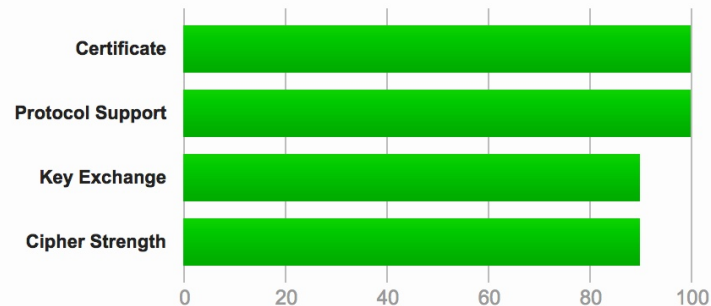
SSL Report: connectcarolina.unc.edu (152.19.220.54)

Assessed on: Fri, 13 Oct 2017 21:09:28 UTC | [HIDDEN](#) | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

The server does not support Forward Secrecy with the reference browsers. Grade reduced to A-. [MORE INFO »](#)

Optimal SSL/TLS Settings

- Recommendations continually evolve, but a couple of starting points include:

- "SSL and TLS Deployment Best Practices"

- <https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices>

- "Applied Crypto Hardening"

- <https://bettercrypto.org/static/applied-crypto-hardening.pdf>

Encrypting Data at Rest

- Encrypting data at rest is often trickier.
- Some sites may do whole disk encryption *when the system is quiescent*, but leave all data decrypted once the system has booted up. That reduces (cough) the utility of things like whole disk encryption for systems that are always live.
- Nonetheless, strive to encrypt everything as much as possible, as routinely as possible.
- Be sure to also think about secure cryptographic key storage (e.g., use a hardware security module when possible). See for example <https://aws.amazon.com/cloudhsm/>

Compulsory Access to Your Data

- Cloud providers may, under some circumstances, be **required to provide government authorities with access to your data**. This may be due to a court order, or as a result of national security program, as was revealed in Edward Snowden's leaks.
- **You may not be notified of government access**, particularly if the order served on your cloud provider prohibits the provider from even disclosing the existence of that order to you.
- As is true for other potential confidential vulnerabilities, your best bet is to use strong encryption so that your cloud provider doesn't have the ABILITY to disclose confidential information in unencrypted form.
- **If you absolutely need to know that no third parties have been given access to your data, you may want to avoid the cloud altogether.**

VII. Cloud Risks:

Integrity

"Well, I've been afraid of changin'
'Cause I've built my life around you
But time makes you bolder
Even children get older
And I'm getting older, too"

Fleetwood Mac, *Landslide* (1975)

Classic Data Integrity Example: Unauthorized Grade Changes

- "University of Iowa suspects grade tampering reason for HawkID security breach"

"The University of Iowa is investigating a “handful” of possible cases of cheating — and warning the entire campus community to change their HawkID passwords — after a faculty member discovered a student’s grade had been changed without authorization. [* * *] According to that notification, the suspects obtained the account information by secretly attaching physical devices to university computers in classrooms and computer labs."

<http://www.thegazette.com/subject/news/education/higher-education/university-of-iowa-suspect-cheating-behind-hawkid-security-breach-20170119> (January 19th, 2017)

Ulowa Is Not The Only Site That Has Been Victimized This Way

- For example: "Easy-to-get hacking device puts KU professors' information in student's hands," <http://www.kansascity.com/news/local/article178522396.html> (October 12th, 2017)
- The culprit is often a tiny USB hardware key logger, surreptitiously installed on a podium computer or other shared system. It lurks there, eavesdropping on usernames and passwords, which get sent off to a hacker's throw away email account or otherwise exfiltrated.
- **If you are not yet convinced that you should be insisting on multifactor authentication everywhere, particularly for cloud-based services, maybe you should reconsider?**
- Remember, if a bad guy can't hack a cloud service, the best option (from the hacker's POV) may be to hack the user of that service...

So What About Data Integrity in The Cloud?

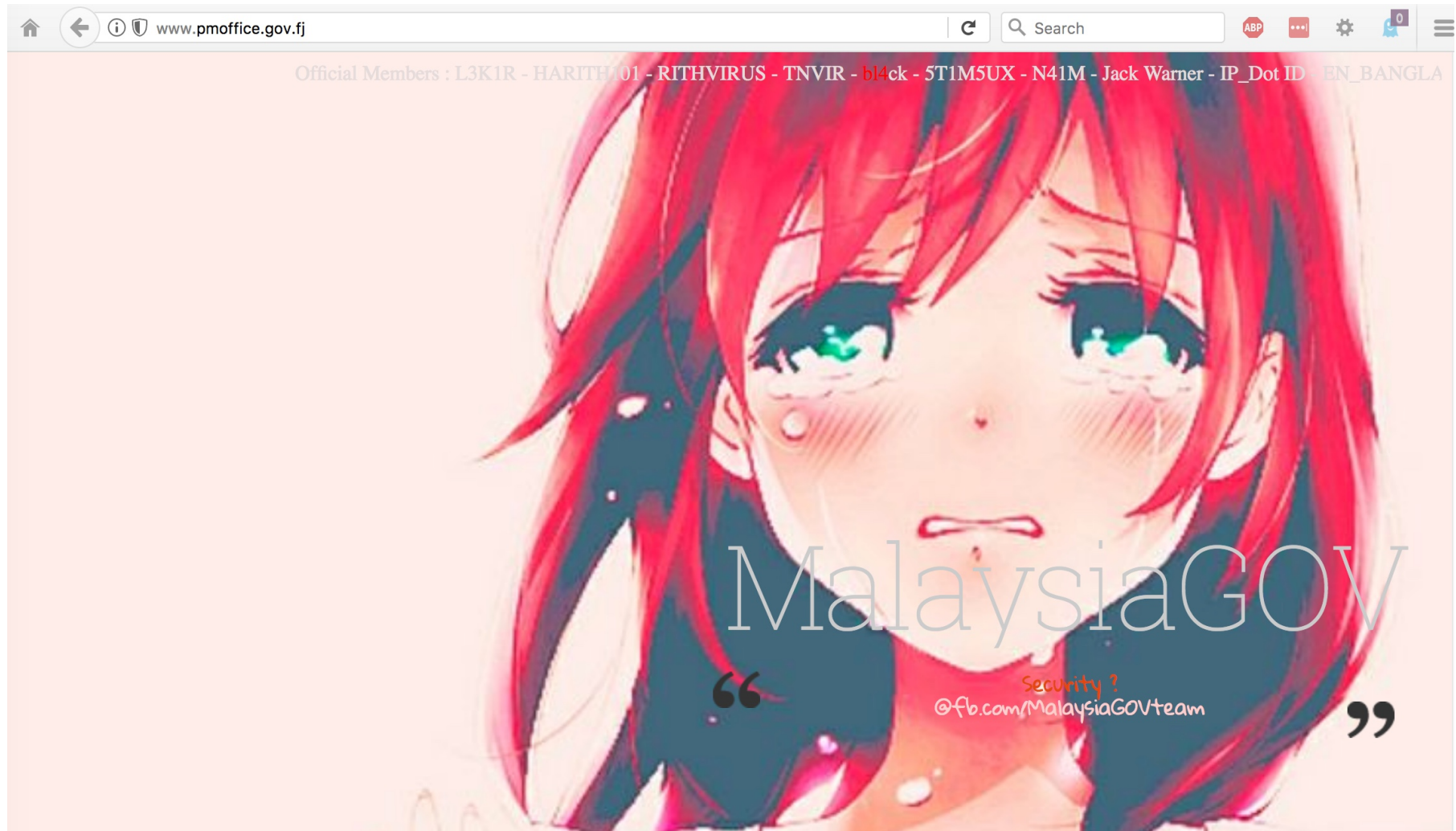
- How do we (rigorously) know that the GBs (or TBs!) worth of files we might have stored in the cloud haven't been changed?
- Some of us may checksum critical **static files**, but do we religiously check those file checksums to ensure that nothing's changed? And what about all the files we DON'T check, eh?
- Or what about large dynamic databases? It can be VERY hard to have high confidence that the contents of those sort of databases are right...
- Some might wonder "Are attacks on data integrity really that common?"
- Sure they are. It's just that often we don't think about it as a "data integrity" or "files being tampered with" issue, we tend to run into it as "sites getting hacked" or "defaced" or maybe systems getting hit with "ransomware" issue.

An Example Of A Site That Admitted Experiencing Data Corruption (In So Many Words)

- [** * **] MJ Freeway told Marijuana Business Daily that the attack was on its infrastructure – main databases and backups, "but no client data was stolen." Later, the company said it might "take two or three weeks to fully restore service to dispensaries and recreational marijuana stores.
- [** * **] Jeannette Ward, director of data and marketing for MJ Freeway, said, **"The attack was aimed at corrupting, not extracting, data.** What that means is all client-patient data is still protected, still safe, still encrypted and was not viewed by the attackers. [*continues*]

<https://www.csoononline.com/article/3157747/security/pot-dispensary-it-director-asks-for-help-after-tracking-system-software-was-hacked.html> (emphasis added)

Sample Website Defacement: www.pmooffice.gov.fj (The Prime Minister's Office, Government of Fiji)



Cloud Data Corruption Often Goes Undetected

- *"In this paper, we present a comprehensive study on 138 real world data corruption incidents reported in Hadoop bug repositories. [* * *] only 25% of data corruption problems are correctly reported, 42% are silent data corruption without any error message, and 21% receive imprecise error report. We also found the detection system raised 12% false alarms [* * *]"*

"Understanding Real World Data Corruptions in Cloud Systems,"
<http://ieeexplore.ieee.org/abstract/document/7092909/>
date 23 April 2015

Recovering From Data Corruption Incidents

- If data corruption incidents DO get detected, the most common approach to recovering from data corruption/unauthorized file modifications is to **restore data from a trusted backup**. When you're running systems locally, you also probably arrange for them to be backed up, periodically testing those backups for usability, etc.
- But what about in the cloud? **Are you backing up data that's there, too, somehow? Or are you trusting your cloud vendor to do it for you?**
- Data loss may be more common (and catastrophic) than you think...

Cloud Computing Users Are Losing Data, Symantec Finds

INVESTOR'S BUSINESS DAILY Investor's Business Daily – Wed, Jan 16, 2013 3:55 PM EST

Email Recommend 18 Tweet Share +1 Print

RELATED QUOTES

Symbol	Price	Change
SYMC	24.63	-0.11



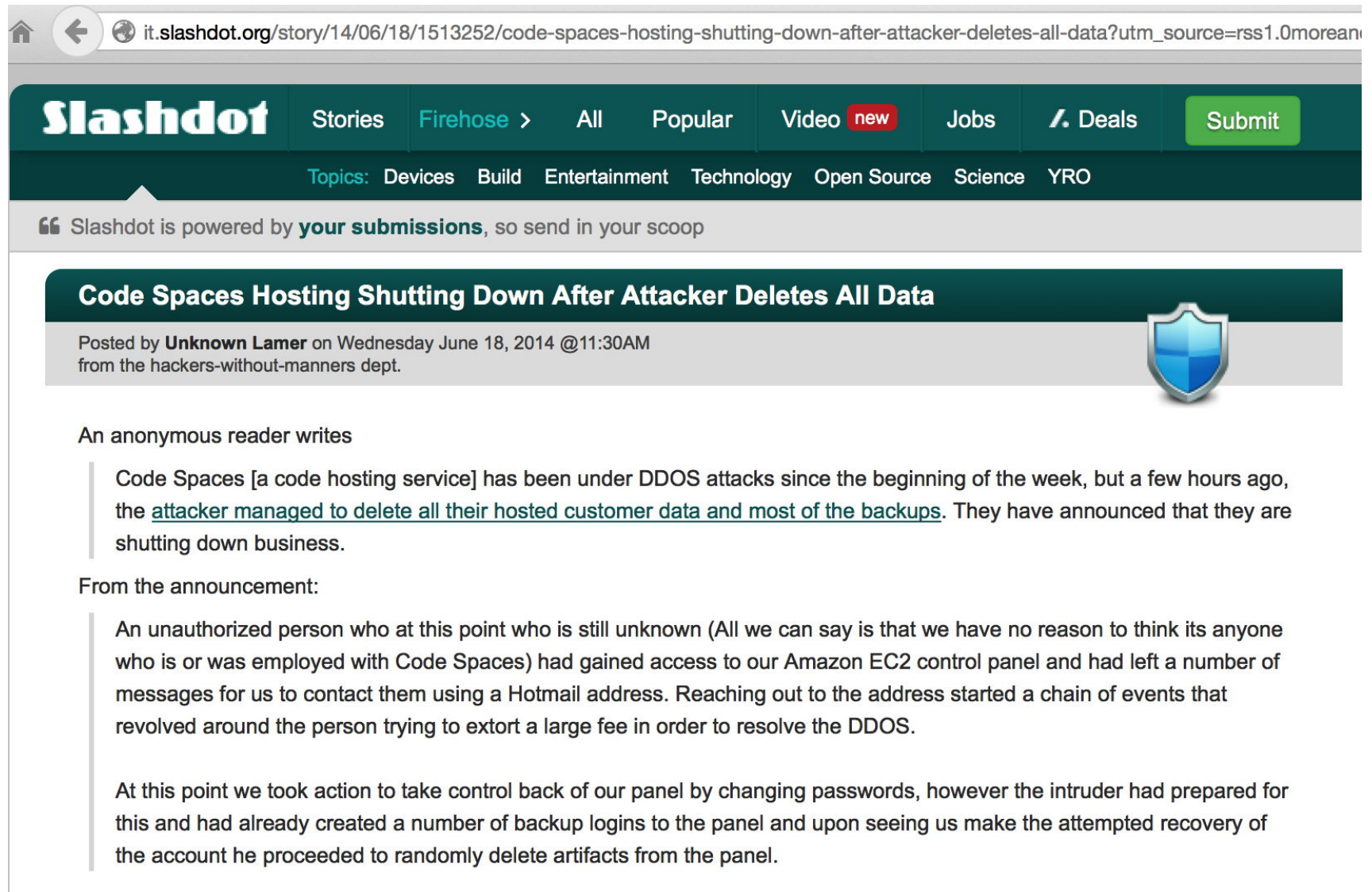
AMZN	297.45	-5.78
-------------	---------------	--------------

Cloud computing is a ticket to losing data for two in five companies, a new study finds.

"It's really kind of astounding," said Dave Elliott, a cloud marketing manager at storage and security company Symantec (**SYMC**). The company polled more than 3,200 organizations to gauge hidden costs of the cloud and ways to mitigate problems.

"Forty-three percent of respondents have lost data in the cloud and have had to recover from backups," Elliott said. And the recovery process has failed at least once for most.

Codespaces: "Shutting Down After Attacker Deletes..."



The screenshot shows a web browser window with the URL `it.slashdot.org/story/14/06/18/1513252/code-spaces-hosting-shutting-down-after-attacker-deletes-all-data?utm_source=rss1.0morean`. The Slashdot website header is visible, featuring the logo and navigation links: Stories, Firehose >, All, Popular, Video new, Jobs, Deals, and a Submit button. Below the header, a banner reads "Slashdot is powered by **your submissions**, so send in your scoop". The article title "Code Spaces Hosting Shutting Down After Attacker Deletes All Data" is displayed in a dark green box, accompanied by a blue shield icon. The post is attributed to "Unknown Lamer" on Wednesday, June 18, 2014, at 11:30AM, from the "hackers-without-manners dept.". The article text begins with "An anonymous reader writes" and describes a DDOS attack on Code Spaces, where an attacker managed to delete all hosted customer data and most backups. The article continues with a quote from the announcement, detailing an unauthorized person's access to the Amazon EC2 control panel and their attempt to extort a fee to resolve the DDOS. The text concludes with the company's response, including changing passwords and the intruder's subsequent deletion of artifacts.

it.slashdot.org/story/14/06/18/1513252/code-spaces-hosting-shutting-down-after-attacker-deletes-all-data?utm_source=rss1.0morean

Slashdot Stories **Firehose >** All Popular Video **new** Jobs Deals **Submit**

Topics: Devices Build Entertainment Technology Open Source Science YRO

“ Slashdot is powered by **your submissions**, so send in your scoop

Code Spaces Hosting Shutting Down After Attacker Deletes All Data

Posted by **Unknown Lamer** on Wednesday June 18, 2014 @11:30AM
from the hackers-without-manners dept.

An anonymous reader writes

Code Spaces [a code hosting service] has been under DDOS attacks since the beginning of the week, but a few hours ago, the attacker managed to delete all their hosted customer data and most of the backups. They have announced that they are shutting down business.

From the announcement:

An unauthorized person who at this point who is still unknown (All we can say is that we have no reason to think its anyone who is or was employed with Code Spaces) had gained access to our Amazon EC2 control panel and had left a number of messages for us to contact them using a Hotmail address. Reaching out to the address started a chain of events that revolved around the person trying to extort a large fee in order to resolve the DDOS.

At this point we took action to take control back of our panel by changing passwords, however the intruder had prepared for this and had already created a number of backup logins to the panel and upon seeing us make the attempted recovery of the account he proceeded to randomly delete artifacts from the panel.

When You Start Looking at Cloud Backup

- Be sure to distinguish between backing up data **TO** the cloud, and backing up what you currently have **IN** the cloud.
- Remember that our worry is "What happens when the data that was IN the cloud that needs to be restored?" Depending on what caused data to be lost or corrupted, some strategies may NOT save you (example: RAID mirrored data can perfectly mirror data corruption caused by an application flaw, right?)
- Some cloud providers have chosen to specifically focus on cloud backup as a core competency, see for example:
<https://aws.amazon.com/backup-storage/>
<https://www.windowsazure.com/en-us/services/backup/>
<https://www.rackspace.com/cloud/backup>

VIII. "Integrating" With The Cloud

"Wenn getanzt wird will ich führen
auch wenn ihr euch alleine dreht
Lasst euch ein wenig kontrollieren
Ich zeige euch wie es richtig geht"

["When there's dancing I want to lead
even if you're whirling around alone
Let yourselves be controlled a little
I'll show you how it really goes"]

Rammstein, *Amerika* (2004)

Authentication

- In addition to the big three issues of availability, confidentiality and integrity, you may also see more subtle cloud-related security issues. For example, some cloud providers may not do a very clean job of integrating with your identity management system (whatever you may be using for that).
- Some providers may want to do something really, really broken, like periodically syncing a copy of your credential store to their systems (ooh, not good, not good at all), or they may want to use your campus LDAP servers (also not a very good model).
- Other providers may try to substitute THEIR own identity management system as a replacement for yours.
- My recommendation? Encourage cloud providers to support Shibboleth (see <https://www.shibboleth.net/>). It's widely used in higher education as well as by the Federal government.
- And INSIST on support for multifactor authentication!

Pen Testing; Working Incidents In The Cloud

- Standard penetration testing processes (which you may use on your own infrastructure) may not be an option in an outsourced environment (the cloud provider may not be able to distinguish your realistic "tests" from an actual attack, or your tests may potentially impact other users in unacceptable ways)
- If you do have a security incident involving cloud-based operations, how will you handle investigating and working that incident? **Will you have access to the logs and network traffic logs you may need? Will you be able to tell what data may have been exfiltrated from your application?**
- What if your system ends up being the **origin** of an attack? Are you comfortable with your provider's processes for disclosing information about you and your processes/outbound flows?

The Log Access Issue Bears Emphasis

- One of the really useful things you get when you run services locally is log files. You get to see how your services are used, and how people (attempt to) abuse it. Hopefully you're doing that local logging to a central log server, and processing that data with a SIEM (security information and event management system).
- Sometimes when you move to the cloud, you may lose access to log files, and that can really hurt when it comes to your situational awareness. A major attack may be going on, and you might not ever know (until it is potentially too late).
- In other cases, logs may be available for "web-based" review, but not for continuous/routine integration with your SIEM.
- In still other cases, logs may be available upon request, but only to help you deal with particular incidents, not for routine review.
- Be SURE you can get cloud log data integrated with your SIEM!

End User Support and the Cloud

- You are probably used to locally supporting users of local applications. One of the trickiest things to get used to is recognizing that in the cloud, support may be someone else's responsibility.
- If a user has a problem, you may not be *able* to answer their question. You may need to refer the user to a cloud provider's support infrastructure, and *that* support infrastructure may be outsourced to a third party overseas.
- Support may suffer, and in some cases that may negatively impact the security of user's work.
- You will also need to learn to live with not being able to have direct access to a ticketing system operated by the cloud provider, so you may not even KNOW what users are struggling with.

Host-Based Intrusion Detection

- While I'm generally not super enthusiastic about firewalls, I am a big fan of well-instrumented/well-monitored systems and networks.
- Choosing cloud computing does not necessarily mean forgoing your ability to monitor the systems you're using for hostile activity. One example of a tool that can help with this task is OSSEC, an open source host-based Intrusion Detection System.

For more information see <https://ossec.github.io/>

IX. Cloud Provider Choice:

"Go With Cloud Provider Foo, Or Not?"

"Everyone knows but they won't tell
But their half-hearted smiles tell me something just ain't right"

Kid Rock, *Picture* (2001)

Choice of Cloud Provider

- Cloud computing is a form of outsourcing, and you need a high level of trust in the entities you'll be partnering with.
- It may seem daunting at first to realize that your application depends (critically!) on the trustworthiness of your cloud providers, but this is not really anything new -- today, even if you're not using the cloud, you already rely on and trust:
 - network service providers,
 - hardware vendors,
 - software vendors,
 - service providers,
 - data sources, etc.

Your cloud provider will be just one more entity on that list.

"Go Ahead With Cloud Provider Foo -- Or Not?"

- Presumably you make comparable go/no-go decisions for **local** technologies all the time:
 - Is the campus data center secure enough?
 - What operating systems should we recommend (or deprecate)?
 - How can we mitigate the risks arising from malware?
 - Is our learning management system FERPA-compliant?
 - Do we need a new policy to deal with unencrypted data on desktops or laptops?
- For **local** stuff, you have myriad sources of local data and advice to help you reach a decision.

By Contrast: Cloud-As-"Tycho Magnetic Anomaly"

- The cloud may normally be represented by a fluffy white blob, but the cloud's is actually more like a "black box." You end up needing to figure out what's happening inside of it without being able to open it up or even touch it.
- Remember Arthur Clarke's *Space Odyssey* books? If not, see http://en.wikipedia.org/wiki/Monolith_%28Space_Odyssey%29
- **Think of a cloud provider as being just like one of Clarke's black monoliths: even though it may have some sort of mysterious force field that keeps you from directly touching it, you still have to decide what it means, if it's safe to have around, and what (if anything) you need to do about it.**
- When you get right down to it, the primary way you're going to do that is by **asking questions.**

The Problem:

Everyone's Questions Are *A Little Bit* Different

- As a cloud provider, you'd like to have a security FAQ or security whitepaper that you could provide to inquisitive potential customers, answering all (or most) of their security questions, however, seemingly, everyone's questions are just a *little bit* different.
- These questions are often going to be ones that require a senior staff person or persons to answer (correctly). Those guys are expensive, and scarce, and already overworked.
- And the questions you may get may be quite probing/intrusive, and the answers might potentially be quite helpful to an attacker. The provider may not WANT to tell people all the intricacies of how they protect their services. (Security by obscurity isn't really security, but that doesn't mean they want to disclose *everything*)

"We'll Review Their Audit Reports, Instead..."

- What exactly will you be looking for? **What would be a "deal breaker,"** if you saw it in an audit report?
- Some new providers may NOT have been audited at all. Getting audited "just for you" may be expensive, and not something they're interested in doing. What then?
- Not all audit reports are the same, so which one(s) do you want? For example, assume your choice is SOC-1, SOC-2, or SOC-3? (FWIW, AWS offers all three SOC reports, and many others see <https://aws.amazon.com/compliance/#third-party>)
- Providers may be reluctant to share a non-redacted audit report with you (although a major potential customer **who is willing to sign an NDA** to get access to an audit report may have better luck than a smaller-scale customer who is not willing to sign an NDA)
- And how often will any audit need to be **repeated?**

"Checking References"

- Asking others who may be using the cloud service may give you some insights into what they've seen, but...
- Your site and the reference site(s) may not have the same infrastructure, or the same planned usage, or the same tolerance for risk, etc.
- Those pesky NDA terms may limit a colleague's ability to candidly share what they've learned (at least "on the record"/for attribution)
- Just like talking to employee references for a new potential employee, you usually end up getting referred only to those who've got nice things to say (for some reason)
- Oral reports are also not very comparable, if you're trying to evaluate multiple potential alternatives side-by-side.

Using a Standardized Security Framework

- If we want to do a systematic review of cloud provider security, maybe it would make sense to use some sort of **standardized security framework**?
- If we could all agree to use the **same one**, a provider would only need to complete **one** framework, and because the framework would be standardized, we could:
 - Be comfortable that we haven't overlooked anything obvious
 - Easily compare the responses from provider A with the responses from provider B
 - Not have to wait while a provider answers a newly written set of security questions
- If we could all agreed to use the same security framework, providers could just complete that one, confident that it would handle the lion's share of the questions from all users.

Whose Security Framework Should We Use?

- Cloud security frameworks have been developed by many agencies/organizations, including:
 - Cloud Security Alliance
 - ENISA
 - GSA
 - ISO
 - Jericho Forum
 - NIST
- Just like "Goldilocks and the Three Bears," some cloud security frameworks may be too simple, other cloud security frameworks may be too complex. The trick is finding one that's "just right."
- **The sweet spot is the CSA CCM.**

X. Cloud Security Alliance Cloud Controls Matrix (CSA CCM)

"I see you've got your list out, say your piece and get out
Guess I get the gist of it, but it's alright
Sorry that you feel that way, the only thing there is to say
Every silver lining's got a touch of grey"

Grateful Dead, *Touch of Grey*

CSA Cloud Controls Matrix

- The CSA Cloud Controls Matrix (CSA CCM) is the security framework that I've previously recommended, and continue to recommend folks use for evaluating the maturity and completeness of cloud provider security programs.
- The CSA CCM approach avoids any problems that may be associated with completing a checklist but NOT FIXING issues that may be exposed as a result.
- If you complete a CSA CCM-based whitepaper talking about your approach to security, it becomes quite difficult to gloss over/ignore areas where obvious deficiencies exist.

CSA CCM 3.0.1

- The current version of the CSA CCM, 3.0.1, which was released in updated form on 9/1/2017.
- It has 133 questions spanning 16 different security domains.
- 133 questions is simultaneously a LOT of questions, yet far fewer than some other assessment instruments.
- We think CSA got the length and scope of coverage about right.

What Controls ("Rows") Are In The CSA CCM?

- To see, download a copy at <https://downloads.cloudsecurityalliance.org/initiatives/ccm/ccm-v3.0.1.zip>
- The 133 "controls" are grouped into 16 topical areas:
 - 1) Application & Interface Security
 - 2) Audit Assurance & Compliance
 - 3) Business Continuity Management & Operational Resilience
 - 4) Change Control & Configuration Management
 - 5) Data Security & Information Lifecycle Management
 - 6) Datacenter Security
 - 7) Encryption & Key Management

[continued on the next slide]

What Controls ("Rows") are in CSA CCM? (2)

- 8) Governance and Risk Management
9) Human Resources
10) Identity & Access Management
11) Infrastructure & Virtualization Security
12) Interoperability & Portability
13) Mobile Security
14) Security Incident Management, E-Discovery & Cloud Forensics
15) Supply Chain Management, Transparency and Accountability
16) Threat and Vulnerability Management
- Many of the items in each of these areas are pretty basic "common sense" items.

An Item From The CSA CCM Threat and Vulnerability Management Section

- **TVM-02, Vulnerability/Patch Management:**

Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g. network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.

What's A "Passing Score" on the CSA CCM?

- For example, does a site need to have all controls perfectly addressed? 90% of them? A majority of them in some form or another? What if they're ALL just TBD/in progress?
- There's no right or wrong answer to any item, and many different approaches could work. A stronger response to one item might offset a weaker response to another.
- Sometimes, just seeing HOW a company responds to a CSA CCM item can be very instructive -- do they take the process seriously? Do they just try to get it out of the way as quickly as they can, treating it as if it were a checklist? Do they have answers that appear to be internally inconsistent?
- Academics understand grading essay exams. :-)

Every Site's Needs May Be Different

- Another reason why there's no "passing score" on the CSA CCM is that what's an acceptable answer to those questions may vary from site-to-site.
- For example, site A may be interested in offering an easy-to-use free application for student recreational use, and they may have minimal security concerns as a result.
- Site B, on the other hand, might want to deploy an application for use by special ed student teachers, triggering significant worries about accessibility, data privacy, compliance, etc.
- Different sites, different requirements, different thresholds for what's acceptable – one uniform "passing score" wouldn't work for all sites.
- Because every site's different, the goal should be to give you at least most of the data you need to make an informed decision, without making you pry it out of the cloud provider yourself.

Another Reality: You May Have Limited Luck Seeking Major Changes From a Huge Cloud Provider

- Cloud providers are all about offering **standardized services at scale**.
- As such, they may not be willing (or even able) to consider modifying their service (or their practices/procedures) to meet your preferences/needs.
- If they did make changes to meet your needs, they might find those changes aren't welcomed by an equal number (or more!) existing customers, customers who liked how the provider traditionally did things. **Therefore, you may need to live with "off the rack" rather than custom tailored offerings.**
- Small entrepreneurial cloud providers, on the other hand may be potentially much more flexible.

XI. Conclusion

"The radio reminds me of my home far away
And drivin' down the road I get a feelin'
That I should have been home yesterday, yesterday"

John Denver, *Country Roads* (1971)

"Take Aways" In Summary

- You now have a better sense of why cloud computing has had mixed uptake to-date: a lot of the hesitation relate to worries about security.
- You understand HOW cloud security can go badly, including challenges related to availability, confidentiality and integrity
- You know strategies for addressing those risks, and understand some of the costs associated with doing so
- You have specific tactical items to check (MFA, SSL/TLS, backups)
- You know the importance of thinking about how cloud services will integrate into your overall ID mgmt and security environment
- You understand that investigating a cloud provider's cyber security can sometimes feel a bit like playing "twenty questions"
- You have learned the value of using a standardized framework such as the Cloud Security Alliance Cloud Controls Matrix

Thanks for The Chance To Talk Today!

Are there any questions?