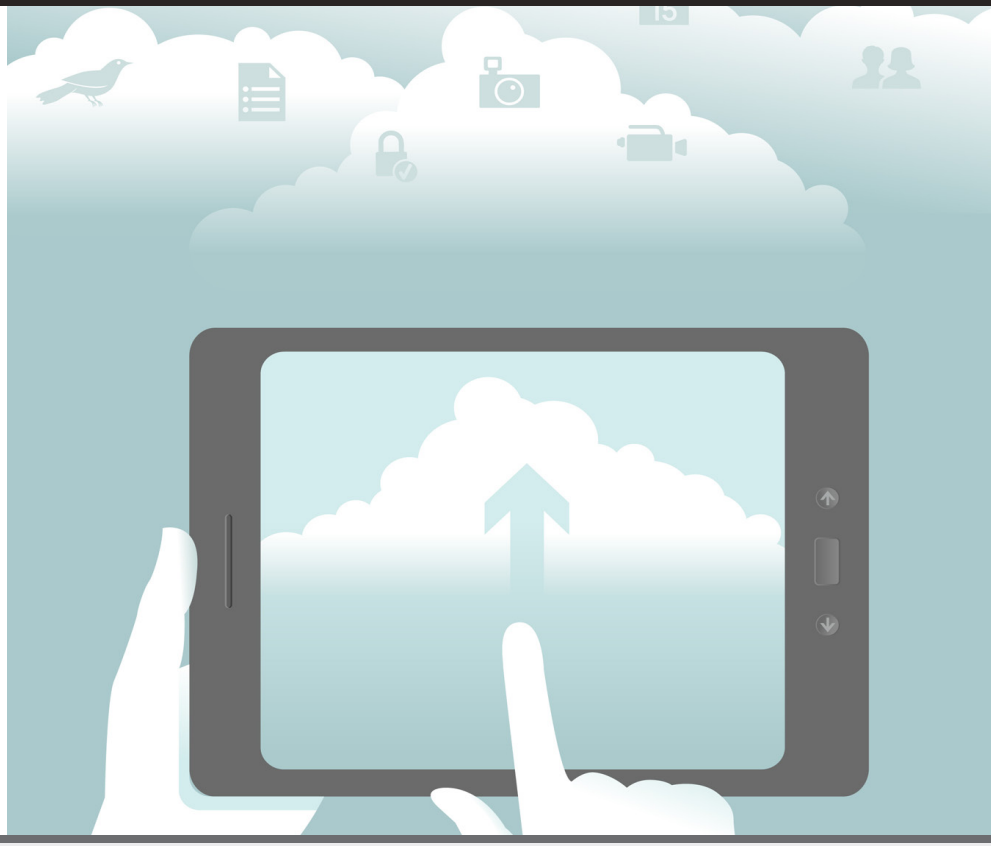
eGuide

IDG Enterprise is CIO COMPUTERWORLD CSO InfoWorld ITWORLD NETWORKWORLD

QTS

presents

Cloud Security



As enterprises ratchet up their use of cloud services, this question is often debated: How secure is data in the cloud? While some believe that moving data to the cloud increases its vulnerability, others feel that, with the right controls in place, the cloud is actually a safer location for storing corporate data than the data center.

In this eGuide, *Network World*, *Computerworld*, and *InfoWorld* examine the issue of cloud security from both sides. Read on to learn how to effectively protect your organization's data in the cloud.

RFC Suggestion: The Responsibility Protocol

Recent security attacks demand new protocols to help improve internet security overall

BY TOM HENDERSON, NETWORK WORLD | Fry me for a catfish. This is an exclamatory used by a dear friend that fits my mood right now. Incredulity. This is a suggestion for the IETF to hand to ICANN, and whatever organization follows them. ICANN are the people that assign names. They're a controversy unto themselves, but a set of Responsibility Protocols might help them regain some of their lost dignity.

Today, there are millions of top level domains, provisioned initially by ICANN and designated name registries. Whether it's .com or .name or .xxx, your name is gold—an asset that ought to be worth something to others. But just because you can register a domain doesn't you have to be responsible for them. This fact, irresponsibility, needs to stop. If you can't be responsible with your loaded gun, you need to have the gun taken away from you.

What kind of bullets are fired from your metaphorical domain gun? Let me dish up a few examples:

The FREAK and Bar Mitzvah RC4 attacks

RC4 attacks permit your seemingly safe https: domain to twist encryption selection to something pretty simple to hack and crack. Somehow, your site still allows for this ancient, dangerous, and easily corrupted encryption algorithm to undermine TLS security. If your site can use it, it can downgrade security in ways you didn't intend, right? Don't want to propagate THAT, do you? No, places like whitehouse.gov wouldn't do that, would they?

Mail hosting irresponsibility

Looking at you, Yahoo and Tom.com. Every domain holder, active or not, needs to have an abuse account to report security or spam abuse. The abuse must then be dealt with within a reasonable amount of time.

This account cannot have a spam filter that prevents a forwarded spam message, hopefully with the mail's headers, from being received. Looking at you, Tom.com. Or maybe you use an obscure RFC to mandate abuse reporting that no one can use, thus sending your mail abuse problems conveniently to zero—looking at you, Yahoo.

Oh, then you have to deal with it. Kill spammer accounts. Yes, you. Yes, now. Yes, noting their IP address, ban them. If it's a user in your domain, you have to shut them off until their bot machine is cleaned so that it can't be used as a spam source. Looking at you, Comcast, BTInternet, to name a few offenders. No active abuse account recipient? Then your domain name should not be renewed until proof exists that an abuse account is both alive and working. Failing this, pull the domain from DNS and route it to a "Sorry, Folks" page.

Skinny security, A/K/A no secondary auth

It's bad enough that sites like United Airlines use POST pages with mixed plain-text and encrypted information, but it ought to

Every domain holder, active or not, needs to have an abuse account to report security or spam abuse. The abuse must then be dealt with within a reasonable amount of time.

be mandatory—if you're taking money or storing private information—to require a user secondary authentication authorization. Token, password, bio-something, key device, I don't care which of these you use, but you must use something. Sessions must time out and demand a new token after 15 minutes of inactivity—and no persistent session without a secondary auth.

Hey, banks—aren't our assets worth something? Yo, Amazon, how about it? Fleabay? C'mon folks, let your users become comfortable with secondary auth so that your fraud costs go down, and your customer love goes UP! A colleague of mine cites an app that will beat a password with three hundred million dictionary attacks per second. While I'm impressed with his hardware, don't doubt that even low-profile targets snap like a twig when attacked in this way. Let's salt it up and make it more difficult.

People could use all of the good stuff in the cloud, if the cloud wasn't a cesspool of hideous, unevenly applied security and rascal hosting sites worthy of being kicked to the curb. I want to trust the cloud. Google, for all of its strangeness, happily offers up and demands a secondary auth, usually a Yubikey, for its employees and contractors. Let's make them demand that of search, too.

For Cloud Security, It's Not the Hackers You Should Fear

Businesses have a lot of control over cloud-stored data, but many don't know how to use it

BY DAVID LINTHICUM, INFOWORLD | When I talk to reporters, they seem to focus quickly on security concerns around cloud computing, especially the public cloud. Mostly they cite recent well-publicized breaches such as Sony Pictures, Home Depot, and more recently, Anthem.

They got hacked, so clouds are more vulnerable, right?

Wrong.

As I've said many times, the degree of security—whether within cloud-based or on-premises systems—is determined by two factors. One is the planning and technology that goes into engineering the security solution. The other is the organization's ability to operate systems in proactive and secure ways.

To be honest, I'm getting frustrated with the constant questions about cloud security. I've learned to respond with a quick question: Why do you think your data is less secure in a public cloud?

Although that response is a bit passive-aggressive on my part, I'm actually interested in the answer. For the most part, the cited reason is that the data is no longer in your direct control, which somehow makes it more vulnerable.

The truth: Although you may not control the data on your premises, you still own and control the data. You may not be able to visit the data center and have lunch in the server room, but you still can control both the data and the layers of security safeguarding it. I've yet to see a public cloud provider that does not allow this configuration. No, your data is only as vulnerable as your security protocols, cloud or not.

Although I don't see massive data breaches in public clouds, I see businesses use public clouds improperly. The largest threat to security is the lack of qualified cloud developers, engineers, architects, and security experts who understand how to make cloud-based systems secure.

Dumb mistakes are much more of a threat than data breaches. As more enterprise systems move to the cloud, we're bound to see more of those mistakes.

Security is determined by two factors: the planning and technology that goes into engineering the security solution, and an organization's ability to operate systems in proactive and secure ways.

Encrypted Data In the Cloud? Be Sure to Control Your Own Keys

Data encryption in the cloud is an absolute requirement these days. When you talk to your service providers about encryption, be sure to specify that you want to control your own keys

BY LINDA MUSTHALER, NETWORK WORLD | With cloud computing there's no longer a question about whether you should encrypt data. That's a given. The question today is, who should manage and control the encryption keys?

Whether talking to an infrastructure provider like Amazon or Microsoft, or a SaaS provider, it's imperative to have the discussion about key control. The topic is more relevant than ever as more companies move regulated data into the cloud and as concerns about data privacy grow.

Protecting regulated data is top-of-mind in the U.S. where regulations such as PCI and HIPAA dictate that third parties not be able to access an organization's sensitive data. Even if the data is strongly encrypted, it's a compliance compromise if a cloud service provider has access to a full key that can decrypt the information without the data owner's knowledge or permission.

European countries, especially Germany and France, are more concerned with data privacy. They are troubled by the fact that U.S.-based cloud vendors can be subpoenaed by the U.S. government to provide access to specific information, even if it resides outside the United States. Last April, Microsoft was ordered to hand over a customer's emails to U.S. authorities, even though the data was held in a data center in Ireland. If Microsoft also held the data's encryption key, the vendor could be compelled to provide that to authorities as well.

When it comes to processing and storing data in the cloud, organizations need to control their own encryption keys. What's more, this ownership must be established before contracting for a cloud application or platform.

The imperative for encryption for data in the cloud grows stronger every day—for security, for compliance, for privacy, and for peace of mind. Organizations that are putting their data in the cloud need options in which they control the encryption keys.

The imperative for encryption for data in the cloud grows stronger every day—for security, for compliance, for privacy, and for peace of mind.

IT Needs to Stop Pretending It's Not Responsible for Cloud Security

Public cloud apps are the new mainstream; IT can't keep pointing fingers or closing its eyes to avoid responsibility for securing them

BY KEVIN FOGARTY, COMPUTERWORLD | Corporate IT departments have lost the fight against cloud computing, but continue to put their companies at risk by refusing to secure the intersection of the cloud they can't stop and the enterprise they have to protect.

The fight over public cloud, if there ever really was one, is over. Thirty-eight percent of end users admit deliberately using non IT-approved cloud apps because getting approval from IT is too difficult, according to a GigaOm report.

But 81 percent admit using unauthorized Software-as-a-Service (SaaS) apps. 81 percent!

One user who does something dangerous is a security problem. One percent of users doing the same thing is a persistent internal threat. Thirty-eight percent is a massive, dramatic failure to help users get their work done in the way the company wants them to do it. Thirty-eight percent should get a lot of CIOs fired.

Eighty-one percent means it is, effectively, everyone. Eighty-one percent means the war was lost so long ago the winners don't remember why the losers are still complaining.

The GigaOm report—based on the results of three previous GigaOm surveys and co-sponsored by enterprise cloud-services security provider CipherCloud—urges enterprise IT departments to embrace Shadow IT and make some accommodation with the cloud that will make it safe to use.

But 81 percent means "shadow" IT is real IT, and the IT department better get on board with its priorities right quick.

Most IT departments can't even see cloud apps. IT managers told Cloud Security Alliance pollsters their companies use fewer than 10 cloud apps; traffic analysis from Netskope showed the real average is 579.

Except... IT's cloud blindness seems only to apply to end users, not to itself. According to a November, 2013 Frost & Sullivan survey, 91 percent of IT departments use SaaS apps that have not been approved by IT, while only 83 percent of individuals working in IT use non-approved SaaS apps.

So whole IT departments will use public cloud for their own work, but refuse to update perimeter security or network monitoring enough to let them see web apps, let alone encrypt that traffic and possible secure them? Who is supposed to do that, if not IT?

Thirty-eight percent of end users admit deliberately using non IT-approved cloud apps because getting approval from IT is too difficult.

Seventy-nine percent of IT people polled by Forrester in May of 2014 said end users should be primarily responsible for securing data in the cloud. That doesn't mean IT thinks users are responsible; no one in IT thinks users are responsible. The survey said IT people think users should be held responsible if something goes wrong, which is a great way to blame someone else ahead of time for a disaster that IT knew was inevitable and could have prevented.

Which means that IT knows as much as it needs to about cloud and is just avoiding it to keep from having to be held responsible, which is unacceptable. Regardless of whether IT approved the tools employees are using to do their jobs or not, IT is responsible for the security of the company's IT infrastructure and data even when the threat is coming from sources of which IT disapproves.

IT has lost that battle. It's time to step up and fix the security problem.

Luckily, since we're talking about the cloud, no one has to actually fix the problem; they only have to hire someone from outside who will.

No one suggests cloud security is perfect or that services are available to fix every problem, but there are lot of cloud security choices available. The one choice IT does not have is to continue doing nothing to secure the junction of the cloud and the enterprise. Users have voted; IT lost. The cloud is part of the enterprise and IT is responsible for making sure it's secure.

Finger-pointing is a problem, not a solution.

8 Steps to Secure Your Data Center In the Distributed Computing Era

Today's dynamic computing environments require a more flexible and adaptive approach to security; here's how to get there

BY INFOWORLD STAFF | It's no secret that information security has failed to keep up with the speed of business and IT. While data centers have become increasingly dynamic, accommodating rapid application changes and on-the-fly deployments that span private and public clouds, security has remained relatively static, based on perimeter appliances like firewalls or other network chokepoint devices that leave the insides of the data center vulnerable to attack.

In addition, security policies are tied to network parameters like IP addresses, ports, subnets, and zones. As a result, security is highly manual, potentially error-prone, lacking visibility inside the perimeter, and inflexible to changes like cloud migrations or application and environment changes. Enterprises should consider the following strategies to make their security more adaptive to the demands of rapidly changing computing environments:

1. Anticipate workload changes, additions, and movements

In many enterprises, deploying new applications, changing existing applications, or migrating applications to the cloud requires significant effort for security teams because so many systems—from firewalls and VLAN configurations to cloud security systems—must be modified. Enterprises need security built around the context of application workloads (their properties, environments, and relationships) rather than the underlying infrastructure. Such an adaptive security strategy can automatically provision just-in-time policies based on application changes such as the launching of new workloads (as part of an autoscaling operation), application migrations, and environment changes.

2. Audit your applications' interactions

Enterprises generally lack visibility into the east-west traffic between application workloads in their data centers and public cloud environments. They need a graphical view of multitier applications based on the traffic flows between the individual workloads that make up the applications. This application topology view can provide a complete picture of north-south and east-west interactions, chatty workloads, and connection requests from external entities that are not authorized. Better still, if the application topology map is interactive, security teams can drill

Security policies are tied to network parameters like IP addresses, ports, subnets, and zones. As a result, security is highly manual, potentially error–prone, lacking visibility inside the perimeter, and inflexible.

down for details on the specific context of a workload and its relationships with other workloads. This can help security teams design accurate and well-informed security policies based on application needs.

3. Assume that attacks are inevitable

Very often, enterprises invest in strong perimeter defenses, then assume that the workloads behind the perimeter are secure. Yet most data breaches involve attackers who have made it past the perimeter and compromised one server. The attackers then fan out inside the data center to other vulnerable systems, finally making away with sensitive data. Enterprises need security inside their data centers that can lock down interactions between workloads to permitted communication paths and prevent unauthorized connection requests.

Cyber attacks are rarely the result of the compromise of a single server or endpoint. Even if a single workload is compromised by a bad actor, the data center security strategy should prevent the lateral spread of that attack to other systems. Such a reduction in the attack surface can also help the recovery of systems because individual workloads are fully isolated from the larger environment.

4. Future-proof your application deployments

Security teams are often concerned about the lack of control over the network in cloud deployments. Most data center security strategies are dependent on the network, which means that the security for applications in private data centers is often very different from security for applications in the cloud. This leads to divergent security strategies that need to be tested and maintained. Enterprises must pick security strategies that can be consistent across private data centers and public clouds. After all, the expected application behavior and its security needs don't change based on where it runs.

5. Choose security technology that is independent of the infrastructure

Security that is designed for a specific computing environment does not account for the dynamic nature of today's computing environments where virtual servers can be launched on demand anywhere and applications can be deployed or changed at will. It is important to develop a context-aware security strategy that can protect application workloads with no dependencies on the underlying network or computing environment. Moreover, with data centers running a heterogeneous mix of bare-metal servers, virtual servers, or even Linux containers, security that is agnostic to the computing environment can help provide a consistent security strategy that's easy to deploy, easy to maintain, and less prone to errors.

6. Eliminate the use of internal firewalls and traffic steering

Security that relies on traffic steering through chokepoints or perimeter appliances ties security policies to IP addresses, ports, subnets, VLANs, or security zones. This results in a static security model that requires manual changes to security rules every time an application changes or new workloads are launched—leading to firewall rule explosion and increasing the chances of human error.

Security that can adapt using the dynamic context of workloads decouples security from the underlying network parameters and allows changes to occur without affecting security policies. In a context-aware system, security policies can be

specified using natural-language syntax instead of IP addresses. Further, the ability to enforce policies at the level of individual workloads provides more granular control to administrators.

7. Use simple, on-demand encryption of data in motion to protect interactions between distributed, heterogeneous apps

In distributed computing environments where application workloads need to communicate across both public and private networks, encryption of data in motion is a necessity. IPsec connectivity can be used to encrypt the communications between application workloads. But while IPsec provides permanent, application-agnostic, encrypted connections between nodes, it is also difficult to set up and maintain. Adaptive security solutions can provide policy-driven IPsec without the need for additional software or hardware. This allows security administrators to set up on-demand encryption of data in motion between application workloads running anywhere.

8. Develop strategies to integrate security with devops practices

Devops practices combine agile development practices with IT operations to accelerate the pace of application rollouts and changes. Unfortunately, static security architectures prevent businesses from taking advantage of the potential for continuous application delivery. Adaptive security architectures provide integration with automation and orchestration tools to roll out security changes as part of the continuous delivery process. This allows security and devops teams to build security into the application right from workload inception and to maintain it all the way to workload decommission.

Your security strategy should mirror the dynamic and distributed nature of today's infrastructure and applications. Consider these steps to designing an adaptive approach that can improve your security posture and make security a business enabler.

Can the Enterprise Allow Employees to Use the Public Cloud?

Does your organization allow users to use public cloud tools?

BY TOM HENDERSON, NETWORK WORLD | The theme today isn't about enterprise clouds that are my normal topic, but instead, clouds where end users fly. Face it—your users are in their own clouds. Is that a nervous tic I see on your face?

iCloud OwnCloud
Dropbox
Magic sauce
Store my files
Store your files
Store our files
Mix them all together
Stir with random care
You said that file is where?

I find this harrowing. Users face no real way, without a lot of work that they're disinclined to do or even understand, to know if a personal device's files will be stored securely in any particular cloud provider's bin.

There are no standards. No seals of approvals worth spit. Random selection will take place, with a bias towards something your operating system provider conveniently provides.

Or maybe the home machine is a Mac (see: iCloud) and the office machine runs Windows 7, and the phone is an Android. People interchange files frequently from one device to another without thinking about the ramifications of a differing cloud provider. More copies are better, of course, because people want the convenience of just getting their files, photos, music, videos, and yes, work products, on demand. Demand is for now, not hauling out another device, booting it up, waiting for a logon, logging in (too many machines don't require passwords), maybe a signal, then maneuvering to some deep folder to fetch a file. Convenience rules.

This flies in the face of the hopes, dreams, and practical realities of security officers, policy makers, and IT professionals everywhere. It also explains the successful business model behind every convenience store in the world—time pressure.

There are ways to keep sensitive data from finding its way into someone's messy cloud cache, ranging from draconian to astute. Much depends on the values an organization imposes on its users. Yes, they have to be based on trust, and yes, people—even organized and thoughtful people—can be messy with data assets.

Sophisticated data loss prevention schemes are in place in

People interchange files frequently from one device to another without thinking about the ramifications of a differing cloud provider.

some environments. Others force users to logon to virtual sessions and work within the ostensibly safe boundaries of those sessions. Some use sophisticated document or work-product tracking. Others force and use seriously sophisticated, often OS-based, policy controls (ex: Microsoft's Group Policy Objects) in an effort to impose moats around applications and, hopefully, their data. Swimming moats gets an airborne drone when clipboards are enabled...a trick I've had recently demonstrated to me.

Can you implement an approved cloud? How would you judge it? Encryption on the wire in addition to in-storage? Who do you whitelist?

My values, and those of most of my colleagues, say not to allow any organizational data to end up stored in places we don't control and can't audit—period, end of page, and job, if we catch you. Like BYOD, I also recognize that users will be users, and policies vary on the issue from draconian (yeah, you're fired) to "this is our list of approved sites." Don't use XY or Z, as they're unapproved, meaning blacklisting cloud storage.

If you get a chance, tell me which you—or your employer—might approve of, and why, in three sentences or less. You can also say things like: "No Way, I'll be shot at dawn if I say this, but..." and/or if they would (Upworthy alert) Change This One Thing.