Security in "the Cloud"

By Michael Kemps, CEO

Concerns are occasionally expressed around "the cloud" and ensuring that technology environments are secure. In this age, where it seems that every day we hear about yet another hack, high-profile email leak or the loss of critical information, our focus as IT professionals increasingly falls on security.

Our team selects and supports cloud solutions utilizing best-of-breed providers for infrastructure and messaging. These mainstream providers each invest in their own security platforms. We believe that the security investments made by top-tier providers far exceed any one organization's ability to manage, control and afford.

We have long emphasized the need to secure networks utilizing a multilayered approach. The basis for this begins at the egress of the network, where the environment is exposed to the outside world, and continues into the internal environment, to include employee education, management and socialization. In a traditional self-hosted environment, this means beginning with a top-tier Internet service provider (ISP) and next-generation firewall(s). Appliances, operating systems and applications must each be configured and protected. Policies and documentation must be implemented, tracked, updated and enforced for success.

Extending locally hosted infrastructure to a cloud provider adds extra layers of complexity and shared responsibility. We must become familiar with the provider's facilities, physical security, infrastructure, storage, network and virtualization layers. We must insist and ensure that the environments and associated services are secured. They should be certified and validated by third parties.

Physical Security

Best practices demand only allowing data center access to approved employees and contractors that have legitimate and approved business needs. Access is controlled via presentation of identification and validation that each employee or contractor is authorized. Physical access must be controlled both at building egress and utilizing electronic means: video surveillance, intrusion detection systems and multi-factor authentication technologies are cross-employed.

Network Security

Cloud providers employ methods to protect against distributed denial-of-service (DDoS) attacks, generally utilizing multiple ISPs as well as proprietary mitigation techniques. Limitations control man-in-the-middle (MitM) attacks, IP spoofing, port scanning and packet sniffing, in conjunction with contractual agreement(s) around acceptable use policies for customers.

Connecting the existing on-premises infrastructure to the cloud provider is accomplished via an encrypted connection. A logically isolated area is dedicated to the client. With this extension of existing infrastructure, existing security services, such as firewalls and intrusion detection, continue to be supported. Cloud-based services may extend these services further.

Isolation and Encryption

Hypervisors, instances and associated operating systems should be isolated and protected. Firewalls should generally exist between physical network interfaces and instances, thereby protecting instances. No direct access to physical

infrastructure is provided, and encryption methods protect instances, operating systems and storage from access from both the cloud provider's employees and any third parties. Data encryption is employed both in transit and at rest. Encryption key access is logged and tracked.

Redundancy

Well-designed environments provide redundancy for networking, computing and storage. Cloud providers employ multiple physical and logical locations that allow for regional and distance-spanning recovery of computer and storage capacity. The power and convenience of extending a data center with redundancy that crosses geographical regions with reasonable cost massively improves the speed at which we can recover from technology failure and loss of data.

Desktop as a Service

Some cloud providers extend their infrastructure offerings to include desktop as a service (DaaS). These remote desktops are typically secured and encrypted within the provider's environment, ensuring compliance with security policy requirements. Data is neither sent nor stored on end-user devices. Best-in-class providers integrate the desktop environment with Active Directory and domain services, ensuring continued enforcement of policies, including those that restrict the utilization of local storage device(s).

Change Management

An often overlooked component in the security and reliability of an environment is change management. Top-tier providers apply a systematic approach to ensure that customer-impacting aspects of services are reviewed, tested and approved in accordance with validation and specific requirements. Unauthorized changes are detected and tracked to resolution.

Rapidly transitioning environments, including dedicated resources and hybrid deployments utilizing the cloud, require the development of relationships with top-tier providers. We depend on these organizations to secure and certify the environments that support our businesses on a daily basis.

Careful consideration of physical and network security, isolation and encryption, redundancy and change management is critical to successfully protect your data. Properly architected solutions utilizing top-tier cloud providers can equal or likely even be superior to internally hosted environments. Fear not the transition: education and validation are the keys to success.

About Innovative Computing Systems, Inc.

Innovative Computing Systems, Inc. has focused exclusively on the technology needs of law firms since 1989. The company services large and midsize firms in California and across the United States and takes a best-of-breed approach to all of its offerings. Innovative Computing Systems selects only premier technology partners to provide solutions to its clients and is committed to maintaining long-term strategic relationships with clients to ensure the highest levels of success with IT initiatives. Learn more by visiting www.innovativecomp.com.

P 1.800.541.0450 **E** sales@innovativecomp.com **W** www.innovativecomp.com
Los Angeles | San Francisco | Austin
@ICSGetsIT