CRIME IN THE CLOUD

How Cybercrime Affects Businesses Using Cloud Computing Services

MANAGED CLOUD SOLUTIONS FOR YOUR BUSINESS

CONTENTS

iNSYNQ

EXECUTIVE SUMMARY

Many businesses turn to cloud computing as a way to safeguard company data, but it is not without risks. Moving data to the cloud provides protection from risks associated with in-house computing systems; however, it opens doors for a variety of new security risks created by a shared environment and vulnerabilities created by moving data across a wide network of applications and locations.

Although the cloud environment has become increasingly hospitable to cybercriminals of all kinds, small and medium-sized businesses shouldn't avoid taking advantage of the many, and very real, advantages offered by cloud computing services at every level. The most effective safeguards against crime in the cloud need to come from the cloud, so partnering with a trusted cloud provider can provide protection from cyberattack.

CLOUD COMPUTING BENEFITS BUSINESS

Cloud computing—storing data and apps on remote servers, rather than within a local or in-house system—offers significant benefits for businesses of all kinds, regardless of their size. Within cloud computing, companies can choose from service models such as software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). These solutions offer everything from simple data storage to systems management and more.

Cloud services can help businesses save money, expand services, build brand awareness, and work more efficiently. Hosting company data on remote servers makes it easy for all authorized users to have access, regardless of location, time, or other circumstances. Company data is always backed up and protected from the types of problems that beset local storage, ranging from natural disasters to ransomware attacks. In addition, cloud providers offer a full slate of services for managing that data to meet a company's specific needs.

CLOUD STORAGE REDUCES IN-HOUSE THREATS

A major benefit of cloud storage is the ability to protect data from a variety of in-house security risks, including:

RANSOMWARE THREATS

One important benefit of cloud storage is its protection against ransomware attacks that lock a user's data until a "ransom" is paid or destroy it outright. With important data stored remotely and available for instant access, ransomware threats on in-house systems are neutralized, so that no data is lost or destroyed.

FAILURE OF LOCAL STORAGE AND BACKUP

Local storage systems, including in-house storage backups, can fail for a number of reasons. Natural disasters or system failures can take many company functions offline for long periods of time. Storing data remotely can keep all aspects of a company's online presence available without interruption.

INTERNAL THREATS

Hacking and other malicious misuse of data may not come from outside sources, but from unethical or angry employees, disgruntled former employees, contractors, and other people close to the company who have been given legitimate access to data. Storing data in the cloud can make it easier to block this kind of activity and recover any data that might have been lost.

ACCESSIBILITY OPENS DOORS TO CRIME

Remote storage, easy data sharing among multiple users, and shared servers and technology are among the conveniences of the cloud. But criminals love them too, because those features offer openings for cybercrime.

From simple "phishing" schemes to a massive malware attack, cybercrime can strike anyone, anywhere, from a single home computer to an international retailer's massive bank of customer transaction systems. Many of these crimes are directly "abetted" by the features of the cloud, with serious implications for the health of businesses relying on cloud services to protect their data.

It's possible to purchase a cyberattack capable of shutting down an entire network for a mere $150; that kind of attack becomes possible by creating a network of shared computers carrying the same kind of malware. Although cloud computing offers unprecedented opportunities for a business to streamline services, save money, and expand its reach, the very features that make those things possible may also create vulnerability to a variety of cybercrimes.

Remote Third-Party Storage

In all cloud storage models, data is entrusted to a third party and hosted on its remote servers. That benefits businesses in many ways, such as saving the costs of in-house IT and hardware, but it also means that company data is placed in the hands of a third-party cloud service provider—and not all cloud service providers are trustworthy.

Virtually any entity with access to server space and the basic tools for setting up a business can offer cloud computing services ranging from simple data storage to a full infrastructure. Some companies exist solely as a front for exploiting the data stored by its customers. Others offer low cost services without essential security protections, or fail to keep data secure at the many vectors that make it more vulnerable to hacking.

Multiple Users and Accounts

Multiple users, poorly maintained accounts, and lapsed permissions can leave a company's data vulnerable in cloud storage. These kinds of risks can happen in-house, too, of course. But when data is housed in the cloud, the number of people who have access to it grows. Along with company staff, a number of others at various levels of the cloud provider network will also have access to some, if not all, of a company's sensitive data—and these users may not be trustworthy, even if the provider itself is safe.

Shared Space and System Crosstalk

Depending on the kind of cloud services a business chooses to use, its data typically occupies space with other tenants on shared servers, and some of those users may not be safe—or they may even be cybercriminals. Similarly, data can be moved between servers or levels of service, creating multiple vectors where it can be hacked or damaged as it moves through the cloud hosting ecosystem.

Those vectors, along with the crosstalk between shared elements needed to maintain the data, open doors for hacking, malware, and the hijacking of essential services, in which a user loses access to parts of the data or certain aspects of its business.

CYBERCRIME IN THE CLOUD

Cybercrime experts point out that although cyberspace today isn't necessarily less safe than in previous years, cloud computing in some ways creates an ideal environment for cybercrime to flourish.

Account Hacking and Data Theft

Although many high-profile incidences of account hacking and data theft in recent years have involved direct attacks on a company's own databases, the cloud can make account hacking easier and more difficult to track. With multiple users and shared servers, cloud computing creates a wider network of vectors at which data can become vulnerable. And while identity theft still tops the list of reasons behind account hacking, other motives can also apply, such as sabotage by a competitor or in protest of a company's policies or practices.

DDoS Attacks

Distributed Denial of Service, or DDoS attacks, can shut down a website indefinitely. In a DDoS attack, multiple compromised systems are networked to flood a targeted site with unwanted traffic, shutting it down for as long as the attack continues. Cheap and easy to implement, DDoS attacks can be initiated at any point in the network of applications, infrastructure, and platforms offered by cloud service providers and implemented by multiple users who may not be trustworthy.

API Security Risks

Application Programming Interfaces (APIs) are an integral part of cloud computing services. While APIs allow users to manage and interact with a variety of cloud-based services, using them efficiently requires many permissions and credentials, all of which can open doors for breaching the security of an API. When API keys are stolen, a company's data can be compromised or destroyed from any point in the system.

Shared Technology Risks

Because cloud computing depends on a complex network of servers, platforms, and shared infrastructure, when one part of the system is compromised, it can affect others. A malware attack initiated on one "tenant" of a shared server can easily affect others, thanks to the shared technology that keeps the entire system running.

BEATING CRIME IN THE CLOUD—WITH CLOUD SERVICES

Cybercrime can strike any Internet user, anytime. But the conveniences that the cloud offers legitimate users can also be exploited in a variety of ways that can make businesses more vulnerable to criminal activity on a number of levels.

There are many things a company can do in-house to reduce the likelihood of cybercrime. But the best protection from cloud-based security threats comes from within the cloud itself.

An experienced cloud service provider with a history of excellence in data management and cybersecurity has the resources and expertise to identify and thwart criminal activity that could threaten the safety of the users' accounts.

Summary

Cloud computing has revolutionized the world of business computing. But the features that make cloud storage and other services appealing to business of all sizes can open doors to criminal activity such as data hacking, account hijacking, and DDoS attacks. Businesses can take proactive steps on their end to protect systems from cybercrime. But protecting data in the cloud requires the resources of the cloud, with security and safe data management provided by a trusted cloud services provider with expertise in identifying and blocking any threats to users' accounts.

INSYNQ: THE GOLD STANDARD FOR CLOUD SERVICES

With a secure platform and white-glove service, Insynq provides customized cloud solutions with enterprise-level security and disaster recovery.

To find out more about Insynq's proven expertise and excellence in specialized cloud services, contact the support team at 866-206-1781 or visit www.insynq.com.

REFERENCES:

- "Cybercrime Moving Into the Cloud Big Time, Report Says.' Network World. 23 Mar 2015 *https://www.networkworld.com/article/2900125/malware-cybercrime/criminals-moving-into-cloud-big-time-says-report.html*
- Graham, Luke. "Ransomware Can Cost Firms Over $700,000; Cloud Computing May provide the Protection they Need." 4 Aug 2017. CNBC Tech Performers. *https://www.cnbc.com/2017/08/04/cloud-computing-cybersecurity-defend-against-ransomware-hacks.html*
- Harfoushi, Osama, et al. "Security Issues and Challenges in Cloud Computing: A Conceptual Analysis and Review." Communications and Network, Vol 6:1 (2014) *http://file.scirp.org/Html/3-6101370_42813.htm*
- Hashizume, Keiko et al. "An Analysis of Security Issues for Cloud Computing." Journal of Internet Services and Applications. 27 Feb 2013. *https://jisajournal.springeropen.com/articles/10.1186/1869-0238-4-5*
- "How to Approach Cloud Computing and Cybersecurity in 2017." Information Age. June 2017. *http://www.information-age.com/approach-cloud-computing-cyber-security-2017-123466624/*
- Mills, Elinor. "Cybercrime Moves to the Cloud." CNet. 30 June 2012. *https://www.cnet.com/news/cybercrime-moves-to-the-cloud/*
- Mills, Elinor. "Prosecutor: Cloud Computing is Security's Frontier." CNet. 10 July 2009. *https://www.cnet.com/news/prosecutor-cloud-computing-is-securitys-frontier/*
- Rashid, Fahmida. "The Dirty Dozen: 12 Cloud Security Threats." 11 Mar 2016. InfoWorld. *https://www.infoworld.com/article/3041078/security/the-dirty-dozen-12-cloud-security-threats.html*
- Ruff, Tom. "7 Reasons Why Cloud Based Security Makes Sense." 22 Mar 2017. GCN. *https://gcn.com/articles/2017/03/22/cloud-based-security.asp*