NXTKey

White Paper on

Cloud Computing Cyber Security

PROACTIVE SECURITY
CYBER MANAGEMENT SERVICES
SECURITY OPERATIONS CENTER (SOC)
SECURITY ARCHITECTURE & ENGINEERING

www.nxtkey.com

For roughly a decade, cloud computing has been steadily on the rise. Moving quickly into a $100+ billion industry, today it is far more unusual to find organizations that do *not* backup data and share files via the cloud than to locate those that do.

But along with this relatively "new found" convenience comes some real dangers, not only to privacy and information security in and of itself, but also in terms of legal and ethical responsibilities - primarily for the entities that are being victimized.

Much of the responsibility for deterring cyber attacks, as well as for how restoration and "damage control" is handled following a breach, falls to the cyber security services that are chosen.

Although there is no way to fully eradicate the threat of a cyber attack, the cyber security services and strategies that are utilized can oftentimes mean the difference between an entity having an ample layer of protection or rather, becoming a virtual sitting duck.

In 2017 alone, there were three major malware (ransomware) attacks that had an effect on businesses around the globe - WannaCry, Locky, and Petya. What many companies do not realize, though, this that anti-virus software - which is often believed to provide the first line of defense for such attacks - really only offers very basic protection, and most such software offers no protection at all from ransomware.

So, how can companies put a cyber security strategy in place that can help to deter a cyber attack from happening and / or to recover from an attack once one has taken place?

The Unique Security Challenges of Cloud Computing

While the benefits of cloud computing are many, including a lower cost of ownership of IT applications and (typically) a faster time to market - which in turn can bring about a surge in employee activity - these "perks" can also bring a long list of potential threats. And many of these can go undetected until it's far too late.

Although consumers and businesses are generally aware that cyber security is a key and growing concern, strategies that worked in the past are no longer viable today. With that in mind, steps must be taken in order to ensure that every stage of the threat lifecycle has been covered.

Today's IT infrastructure is far different than it was even just a few years ago. Now, with so many different services relying upon each other and / or having the ability to be shared, it can be difficult to keep cloud-stored data safe.

Consider services like Dropbox, where a user may have his or her account connected to Facebook or other social media accounts. In this case, if the user's Facebook account is compromised, then the same can also happen to their Dropbox account and in turn, all of the information that is stored therein. This can also include the compromising, or even the deletion, of the user's back-up files, too.

With clouds generally being made up of multiple entities, it means that, just like any other "structure" - virtual or otherwise - no configuration can be more secure than its weakest link. Adding more fuel to cyber criminals' fire is the fact that the link between separate entities can allow for attacks to multiple sites to occur simultaneously.[1]

Best Practices for Approaching Cloud Computing Cyber Security Needs

The primary risks that are involved with cloud computing are mainly security-based. Therefore, the first step in minimizing cloud-based risks is to clearly identify what the primary security threats are.

Certainly, due to the vast amount of information that is stored on cloud services, data breaches are at the top of this lengthy - and ever-growing - list. In addition to the personal, financial, medical, and / or intellectual property information that may become compromised in the event of an attack, the victimized organization can also become the perpetrator of sorts, and because of that, it can oftentimes incur lawsuits or fines, and possibly even be slapped with criminal charges.

Compromised credentials and broken authentication are also key cloud related threats. Here, many developers may even make the mistake of embedding credentials and cryptographic keys into the source code, leaving them in public-facing repositories.[2]

Likewise, security of cloud services can also often be dependent on the security of the API - and, according to the Cloud Security Alliance, this risk can increase with third parties that rely on APIs and build on such interfaces, as an organization may need to expose more services and credentials.[3]

So, when it comes to the mitigation of a cyber attack, where is the best place to start?

Today, next-generation anti-hacking tools are a must. This should be considered in addition to an anti-virus solution, which these days is not nearly enough. This is particularly true in the case of a zero-day attack that cannot be blocked from infecting a system by products that use signature based detection.

Oftentimes, because zero-day malware can target financial information from a system, such as pin numbers and credit card details, in order to better protect against data-stealing malware, the solution should ideally:

- Include a real-time Internet traffic scanner that scans all incoming network data for potential malware threats
- Provide malware detection and removal of malicious code from a system
- Contain online scanning capabilities that detect malicious software from online pages and legitimate websites.[4]

Also, it is essential that individuals refrain from offering administrator privileges to anyone - even if they are a trusted entity. If their account becomes compromised, others can be as well, putting all involved at risk.

It is also key to encrypt all data. While it may sound like encryption is only for hardcore security fans, this is actually a misconception. There is a long list of benefits with encryption - but it must be implemented properly. One way to take this method a step further is to encrypt operating systems or hard drives.

Here, using a full-disk encryption tool is typically best - and ideally one that supports AES (the Advanced Encryption Standard). The AES has been tested and improved, and is now used worldwide by many security vendors, due to its high level of security and optimization.

In order to increase overall protection even further, it is important to ensure that communications are not easily accessible to hackers, as well as to malicious software. Here, it can be beneficial to encrypt online traffic.

In order to use the web, while still maintaining privacy, a VPN, or virtual private network, can be used. This private network is able to spread across the normal Internet space, using its resources to create an encrypted channel that can keep communication safe from interception attempts.

Even so, use of encryption only is not enough to ensure safety of data. Therefore, it is also necessary to keep browsers and operating systems updated with the latest security patches. Oftentimes, online criminals will spread malicious code in order to compromise a user's system by using security exploits to take advantage of vulnerabilities.

So, having the most up-to-date programs and applications is a must. Likewise, security programs should include a real-time scanning engine, meaning that everything that is downloaded is scanned.

Aptly Addressing a Cyber Attack and Its Ramifications

It could be argued that the most important criteria in the security of information is human compliance. But the stark reality is that, even when organizations have a strict information security policy in place, it goes without saying that the rules are not necessarily always followed.

Then what?

Addressing every possible stage in the cyber attack lifecycle is a crucial component in cloud computing cyber security in terms of detecting a possible breach, as well as for reducing - or even preventing - certain vulnerabilities.

This will typically start with answering specific questions with regard to the organization's current security situation, such as:

- Is it feasible to detect critical threats in real time?
- Are the security and IT teams up-to-date with the latest attacker techniques?
- Has the present incident response plan been assessed for readiness and functionality?
- Do all aspects of the present cyber security program integrate with one another in order to provide cohesive defense to an attack?
- How quickly and effectively can the organization respond if faced with a threatening incident?
- Are the entity's cyber security strategies continually being updated in order to stay in line with increased threats?

If the answer to any of these questions is no, then it is time to reassess the organization's cyber security strategy and services.

Taking more of a proactive approach means having a deep knowledge of the threat landscape. By more clearly understanding the techniques and the motivations for an attack, determining the precise risk, as well as key vulnerabilities may then be more clearly defined. Lessening the threat of - or the results of - and attack also entails having the ability and the wherewithal to make more informed decisions, more quickly.

The time to implement a cloud computing cyber security plan is not during an attack, but ideally before any type for threat has ensued. Staying a step ahead of adversaries can then lead to better prevention, as well as a faster resolution if an incident should arise.

About the Company

NXTKey Corporation is an agile Small Business that places emphasis on teamwork and partnership with our clients to produce optimum contract performance. We have refined our solution from experience supporting highly complex Department of Justice (DOJ) environments such as United States Marshals Service (USMS), Justice Management Division (JMD), Office of Justice Programs (OJP) and Federal Prison Industries (FPI).

Our depth of experience allows us to provide IT security support for a wide range of IT General Support Systems (GSS) and major applications (MAs) within the Federal Enterprise and following the guidance in the Federal Enterprise Architecture (FEA) and information systems security support services in accordance with OMB Circular A-130, NIST guidelines and standards, as well as other federal policies and regulations.

We specialize in providing our clients a full range of security services specifically tailored to their requirements. These services include: Certification & Accreditation, Security Architecture, Mobile Security and Governance, Risk Analysis and Assessments, Security Policy and Processes, System Auditing, Security Control Assessment, Disaster Recovery Planning, Contingency Planning, Vulnerability Assessment, Penetration Testing, Physical Security Survey, Information Systems Security Training and Security Program Management.

More information on our website at https://www.nxtkey.com