Table of Contents

Just How Secure Is the Cloud?

Image credit: bestfoto77/Shutterstock

In this article, we discuss the state of security for the cloud and how cloud systems are secured. We also talk about compliance with regulations and standards, as well as firewalls and other tools, to achieve confidentiality in the cloud, preventing and mitigating DDoS attacks and more.

When a business or any other organization switches to a new computing environment, security is an increasing concern. After all, hackers are costing consumers and businesses between $375 million and $575 million per year. Put another way, cybercrime is equivalent to 0.8 percent of the international GDP.

What about at the level of a single company? According to a Ponemon Institute survey of 2,000 executives, hackers cost U.S.-based businesses an average of $15.4 million annually. That number is twice as much as the worldwide average of $7.7 million – but no matter where your company is, you can expect cybercrime to cost your business millions.

With that in mind, how well protected is a public cloud service? If you cannot say at any given moment where your private data is physically located, should you consider it a safe ecosystem?

A key point is that the cloud should not be considered a radical overhaul but a tweak of conventional legacy computing environments. While this distributed computing model has unique challenges and requires its own set of strategies and defenses, the security industry fundamentally understands how to protect data, and infrastructure experts know how to implement the appropriate mechanisms.

In fact, that aspect of security expertise applied to the cloud indicates a major characteristic of the technology that speaks in its favor: It is a back end that is engineered and maintained by personnel who are focused exclusively on cloud systems. Because of this, New York Times deputy technology editor Quentin Hardy once noted that this hosting model was “probably more secure than conventionally stored data.”

Still unconvinced? David Linthicum of InfoWorld has voiced the same perspective, saying that the public cloud is a better place to store data than an on-premise system. Linthicum is fervent in his point of view, arguing that security in the enterprise would improve if IT began to understand how strongly protected the cloud industry is.

Cloud hosting companies have robust security defenses because they know that many people would like to sideline them. They tend to have expertise in systemic precautionary measures, including pattern matching and artificial intelligence.

How cloud systems are secured

Security in a cloud setting is achieved in a similar manner to other computing architectures – with a focus on the specific needs of an agile and dynamic model.

Key steps hosting providers take to secure the cloud include strong enforcement of the perimeters and surveillance – physical barriers including high fences, barbed wire, guards and cameras. These hosts also control access to data systemically, with your workforce, guests and partners separated from mission-critical data. In that context, trained experts apply security mechanisms and practices. Finally, comprehensive auditing of systems occurs at regular intervals.

That last point is particularly important because it gives you a way to tell one cloud host from another. When auditing is performed by independent third-party organizations using recognizable standards, you know that a provider has strong internal protocols and safeguards in place that achieve industrial-grade security management. Let’s look at that element before discussing some of the individual components and strengths of a secure cloud environment.

Compliance with regulations and standards

Probably the most common form of third-party compliance or certification that you see in hosting providers and other organizations wanting to win the business of enterprises is the Statement on Standards for Attestation Engagements No. 16 (SSAE 16) – which comes as a SOC 1, SOC 2 or SOC 3 report. This set of guidelines, released by the American Institute of CPAs, basically gives a company a meticulous step-by-step process to check their system and organization controls (SOC).

A cloud provider that has strong enough mechanisms in place to meet the parameters of SSAE 16 will often want to be audited to prove its compliance – even though this standard is not a legal regulation. Note that while SSAE 16 is not necessary to align with data law for your industry, it does show that your ecosystem is robust and conscientiously designed, which is attractive to anyone looking for systems that require their due diligence for regulatory compliance.

Cloud providers actually do have to meet the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH) if they want to provide systems for organizations that are handling protected health information (PHI). Actually, the Department of Health & Human Services has stated that public cloud can be a compliant setting if the right security mechanisms are in place.

In order to support transactions and processing payments, a cloud provider has to meet the guidelines of PCI compliance. Like SSAE 16, PCI compliance is not a law. However, it does make sense to get this certification as well to ensure you meet stipulations of the Payment Card Industry Data Security Standard (PCI DSS) – standards developed and enforced by the major credit card companies. These third-party confirmations that strong controls are in place should make you feel confident in a cloud host even when you cannot “see” the machine that holds your data.

Firewalls and other tools

A centerpiece of security for a network, whether legacy or cloud, is the firewall. Firewalls come in hardware and software forms. By setting up a firewall, you can have all traffic entering your network abide by certain rules. Inspection and filtration at that level is what gives the boundaries of your network real meaning. A key concern with the firewall is that it is dynamic: You must be able to change direction as the threat landscape evolves. That is why having security experts on the clock at a cloud host can be so valuable.

Other components in place to safeguard systems in a cloud data center include solutions to prevent intrusion, block malware, monitor integrity and log all activity. These tools come from entities such as Trend Micro, through its suite Deep Security.

Achieving confidentiality in the cloud

Within a cloud, a managed firewall appliance makes sure that your information remains private. Firewalls block access as necessary, log activity for review by security pros and possibly shift rules to better protect the system.

Beyond the firewall's work to control access, you also want the data itself to be encrypted, whether in storage or in motion. Through cryptography, you can hide the details of highly sensitive data so it is unusable by anyone who does not have the private key.

Preventing and mitigating DDoS attacks

Distributed denial of service (DDoS) attacks are on the rise. Various mega-attacks from the IoT botnet army created through the Mirai software, open-sourced last fall, drove hacking headlines, but that is just the glossiest of the news. According to Data Center Dynamics, the average cost of a minute of IT downtime is $7,900, amounting to a loss of $474,000 for an hour offline. These costs for downtime are a major reason why a DDoS event costs the typical business more than $2.5 million.

DDoS attacks involve a flood of junk requests aimed at a target to attempt to push that system off the internet. To protect your applications and sensitive data against DDoS, it helps to have an infrastructure spread out geographically. Seamlessly shifting the flow of traffic to a redundant data center is simple for a cloud provider with multiple ones that are widely distributed geographically.

Through edge protection, you can maintain redundancy throughout your network via integration from numerous providers, giving you multiple options for traffic so that the impact of a DDoS attack is confined. Edge protection additionally reduces risk by masking your server's IP address and location.

Keeping pace with astronomical growth

The cloud is now growing an incredible seven times faster than the rest of IT, with businesses of all sizes and across all industries using it to build their businesses. More mission-critical data is now shifting to these systems. Companies typically make these transitions because they want to benefit from cost-effectiveness, speed and flexibility gains. However, these firms are also showing that they are becoming less concerned about the issue of security.

The reason people are becoming more confident in these distributed architectures is that they understand cloud service providers have skills and knowledge on staff that extends beyond the IT protective capabilities most companies have in-house, especially firms outside the technology sector.

The importance of proper management

Professional management is a major part of what makes the cloud or any other IT environment secure. A strong service provider will be able to deploy solutions that meet a company's cost and agility needs while also expertly protecting your data.

If you need managed cloud hosting, by leveraging a strong provider, you can take advantage of security features such as intrusion-detection systems, custom-built firewalls and comprehensive anti-malware protection to achieve ongoing data safety.

Developing a More Secure IoT Policy

Photo credit: LeoWolfert/Shutterstock

Enhance your company’s IoT policy with these security tips.

If you want to remain competitive in the future, you have no choice but to succumb to the rise of the internet of things (IoT). However, even with all of the benefits, it’s becoming increasingly difficult to deny the security risks IoT presents.

IoT security risks: alarming and pervasive

If you spend any time studying cybersecurity and recent attacks on businesses – small and large – you’ll come away from the experience fearful. The landscape is brutal right now, and the intensity and frequency of attacks are expected to pick up in the coming months.

According to the 451 Global Digital Infrastructure Alliance Report published at the end of 2016, endpoint security is the number one IoT security concern for businesses. Roughly 63 percent of respondents reported physical unsecured endpoints as their chief concern while poor authentication of these endpoints followed closely at 55 percent.

When you look at the IoT from a broader perspective, 50 percent of respondents said security was their biggest inhibitor to adopting formal IoT policies. This makes sense, as each additional device a business connects to its network ultimately establishes a new entry point to the network.

According to a study conducted by Fortify, 70 percent of popular consumer IoT devices can easily be compromised by professional hackers. In other words, more devices equal more problems.

Then there's the dilemma of the astronomical proliferation of data. With more devices collecting and storing data, there's more for hackers to steal. There's also more at risk for businesses and individual consumers. As a result, there's a greater need for sophisticated security measures to keep confidential data out of the hands of malicious hackers.

5 tips for making your IoT policy more secure

From a business perspective, you need to come up with a sophisticated IoT security policy that eliminates points of vulnerability, secures data and keeps your organization out of harm's way. Below are a handful of suggestions.

1. Only connect devices when necessary

Just because you can connect devices, doesn't mean you should. Each device you add to your network adds functionality to your business, but it also increases risk. If you don't have a functional need for connecting a particular device, there's no sense in adding the risk.

In fact, you should probably think long and hard about how many devices you allow employees to connect to your network. It might sound like a good idea to let each employee use a smartphone, tablet, laptop, and desktop computer, but slow down and consider the situation. There's already a bunch of inherent risks involved – don't push yourself even further behind the eight ball.

2. Create separate networks

One practical way to protect your business is to create separate networks for different purposes. The classic example of this involves guests in your office. While you might need to offer internet connectivity to visitors and/or customers, do you really want them on the same network that you store confidential files and important data? Creating a secondary network removes some of the risk you face in these situations.

3. Use cloud-based SD-WAN

If you want to secure your mobile users, one of the best things you can do is invest in a cloud-based SD-WAN solution. Some options include built-in next-generation firewall (NGFW) and firewall as a service (FWaaS). Both of these features work together to protect mobile users and locations from external threats – something the IoT makes individual users extra vulnerable to.

Even if IoT devices are unable to be patched, the advanced threat protection features found in a cloud-based SD-WAN solution give your IT professionals the ability to implement virtual patching. This added layer of security can prove to be quite helpful in situations where individual devices are targeted.

4. Practice good password hygiene

Many IoT attacks actually start with a single compromised password that gives a hacker access to other information that can be used to cause further damage. To protect your business from these attacks, better password hygiene is a must.

In addition to creating stronger, more sophisticated passwords, encourage your employees and users to implement unique passwords for each account.

5. Provide proper training for employees

While you might understand what it takes to protect your business from IoT-related threats, it’s entirely possible that your employees are unaware of the external risks facing the company. Training employees on proper BYOD and IoT security will help them understand their role and what can/should be done in certain scenarios.

In addition to conducting employee training, regularly check in and see how things are going. The guidelines will probably need to be updated as factors change, so don't be afraid of refreshing your network's users on proper protocol.

Be prepared to evolve over time

While we've been talking about it for years now, it's important to remember that we're only in the beginning stages of the IoT. When we look back in 10 or 12 years, 2018 will be considered IoT's infancy. Having said that, things are still developing at a rapid pace, and you must be prepared to evolve with the changes over time.

You can't set an IoT security policy and neglect it. If you're serious about protecting your business and keeping data safe, you have to regularly evaluate what's happening within your company, in your industry, and on the larger cybersecurity stage.

If you make a commitment to keeping your policy current, you'll do well. There's no guarantee you won't be attacked, but at least you'll have a proper strategy for handling whatever is thrown your way.

How Crooks Hack Passwords

Photo credit: Portrait Images Asia by Nonwarit/Shutterstock

Cyberthieves have a variety of tools available at their disposal to crack your business's passwords and hack your data. Follow these steps to thwart them.

The use of traditional passwords is a slippery slope for companies these days. A much more reasonable approach is to safeguard proprietary data via things like multifactor authentication, single sign-on services or biometrics. According to security researchers' recent findings, the majority of data breaches that occurred in 2017 revolved around stolen or weak access credentials.

Let's dissect the most common password cracking methods that online perpetrators leverage to hack companies and individuals.

Compromising hashed password files

When cybercriminals obtain an organization's passwords, it's most likely because they were able to steal the password file. There are companies that keep password lists in plaintext form. A more secure tactic is to store password files in hashed form. However, neither technique does the trick reliably enough nowadays.

In a nutshell, password hashing denotes a mechanism of one-way transformation of a password that cannot be reversed to obtain the original string. When an employee tries to log in with their regular password, the authentication module automatically transforms it to hashed form and compares the string against the value stored in the database. If these values match, the login is successful.

Threat actors who gain access to a hashed password file can leverage so-called "rainbow tables" to reverse the hash functions. Since this type of activity requires significant computation power, hackers can use specially crafted password cracking hardware, engage a botnet or rent space from cloud providers.

Furthermore, there are services on the dark web that allow perpetrators to outsource the data processing task. In this case, they can rent the service for a specified amount of time and even get tech support.

Ultimately, any password can be cracked as long as the attackers have time and sufficient resources on their hands. The only question is how long it takes. It's usually a matter of days or even hours, not years as it used to be.

This applies to virtually any password created by a human. Computer-generated passwords tend to be more difficult to crack this way, but they are still less secure to use than multifactor authentication.

A particularly disconcerting element in a scenario with stolen password hashes is that the whole processing and cracking routine is performed on the malefactor's machine. The attacker doesn't need to interact with the target company's infrastructure along the way; therefore, no red flags will be raised. Thousands of passwords can be cracked in hours as long as the crook's computer has enough processing power.

Large-scale attacks using botnets

Cybercriminals can employ botnets to compromise big online services. This technique allows them to try numerous different combinations of common usernames and passwords or ones obtained from dumps of credentials that occur regularly. These lists can be purchased on the dark web at a low cost. They usually originate from database breaches, such as the notorious Yahoo email hack that compromised billions of accounts.

Let's imagine a scenario where a threat actor wants to access email accounts.

Attempts to log into the same account multiple times will generate alerts. To circumvent these security measures, the attacker starts with a list of leaked email addresses and a list of the most frequently used passwords. Then they try to get into each one of those email accounts with one of the most common passwords, generating only one failure per account. A few days later, they try another common password for every email address. By using a botnet for this purpose, the crooks make it look like the login attempts come from different sources.

A good response to this attack vector is two-factor authentication, where you receive a secret code that you need to enter every time you try to log in. Sophisticated technologies like facial recognition and behavioral biometrics are tasked with addressing the issue as well. The use of third-party authentication services like Google or Facebook is another good practice that additionally minimizes the number of passwords you have to remember.

Do criminals already have your password?

When cybercrooks zero in on a person, their starting point is to check whether that individual's login credentials have already been stolen from other services. If so, chances are the same password is used for the account being targeted.

Most users have tens or even hundreds of different online accounts. It is too hard to remember passwords for all those accounts; therefore, people tend to use only a couple of passwords, with some minor variations.

Some people think they are completely secure if they have one very complex password and use it for all their accounts. That's a delusion. In case hackers get that password, all of your information is at risk. It doesn't matter how strong the password is if you reuse it. By the way, there are online resources that allow you to learn whether any of your password-protected accounts have been breached in the past.

Incidents in which hackers use malware and steal the password for one's email account are particularly detrimental. This way, the black hats can log in and reset passwords for other services the victim uses. Also, if a website or in-house enterprise service has no limitation regarding login attempts, they can brute-force the password via a dictionary attack or cracking solutions like Hashcat, Mimikatz, or John the Ripper. When going after a high-profile target, the crooks can conduct some OSINT (open source intelligence) to figure out the likely answers to security questions accompanying password recovery.

Passwords created by humans, regardless of their complexity, happen to be low-hanging fruit for hackers. The technologies for cracking them have advanced significantly over time, whereas people remain predictable enough to generate crackable passwords. That’s a paradigm where attackers win and users lose.

Is your password strong enough?

Unfortunately, most online services follow password strength practices that are way out of date. Their requirements usually boil down to the length of eight characters or more and a mandatory combination of symbols, numbers, and uppercase and lowercase letters. It may take a computer minutes or even seconds to crack a password that meets these criteria alone.

All of this poses a serious challenge to end users and service providers. It’s too hard for the average person to create dozens of unique, long passwords for websites they use, change them regularly and remember all of them.

It is recommended to use the longest possible passwords that online services allow and leverage a reputable password management solution to store them. Furthermore, you should safeguard the vault with a master passphrase that’s about 30 characters long. Make sure it’s not a quote from a novel or anything that can be found on the internet. Importantly, all of your passwords should be generated randomly and make little sense, or no sense at all. If you can remember it and tell it to someone, it’s not a good password.

4 security tips to keep your business safe

Photo credit: wk1003mike/Shutterstock

These days, it's not just internet security. Here are four ways businesses can protect themselves from the latest potential threats.

There's a lot of talk about business performance: how to drive better leads, how to enhance customer care, and all this is great. But what about security? Shouldn't this be a central conversation? How are we keeping our businesses safe and secure from theft, hacking and other malicious behavior? Because we haven't got it figured out.

In a recent study, 78 percent of people claimed that they were aware of the risks of unknown links in emails but clicked them anyway. Clearly, there's a gap that needs to be addressed. In this article, I provide four security tips that will specifically apply to how you can make your business more secure.

1. Make security everyone’s business

The first point relates to culture, and it’s one that can potentially make a huge difference in ensuring your business is secure. Namely, make sure security is a topic that is addressed at your workplace at all levels of staff. Security threats are even more threatening if there’s no education around them. Have regular (at least annual) meetings that educate your staff on common security threats and how they can be neutralized.

Security breaches are often the consequence of people becoming complacent. Regular gatherings that educate and remind will help staff stay vigilant in addressing security threats. Security is not just a matter of strategy or technology; it’s also about making sure everybody feels responsible for keeping the workplace safe.

2. Get the gear

Too often, businesses and business owners fall into the trap of thinking they can handle everything themselves. But sometimes, it’s better to buy or partner than it is to build. Leave security to the professionals who understand its intimate workings so that you can focus on what’s important: the day-to-day operation of your business.

Make sure you have robust and up-to-date software, and get it up and running on all computers housing work-related information. Once the software is functioning, you can simply sit back and let it take care of the nuts and bolts of security for you. Don’t skimp on security solutions either. While there are several free, decent antivirus and other security software programs available, these may not be comprehensive enough to protect your business from all threats. Do the research and commit to the solution that protects your business best – not simply the cheapest or most convenient option.

3. Think comprehensively

Just because we’re living in a digital age doesn’t mean that security simply means internet security. There are numerous levels of security that are important to think about and strategize for.

For example, a business needs to not only have security software but also a good physical security system overseeing the workplace. After all, most threats that exist online can also occur through old-fashioned theft. Make sure your building is also secure.

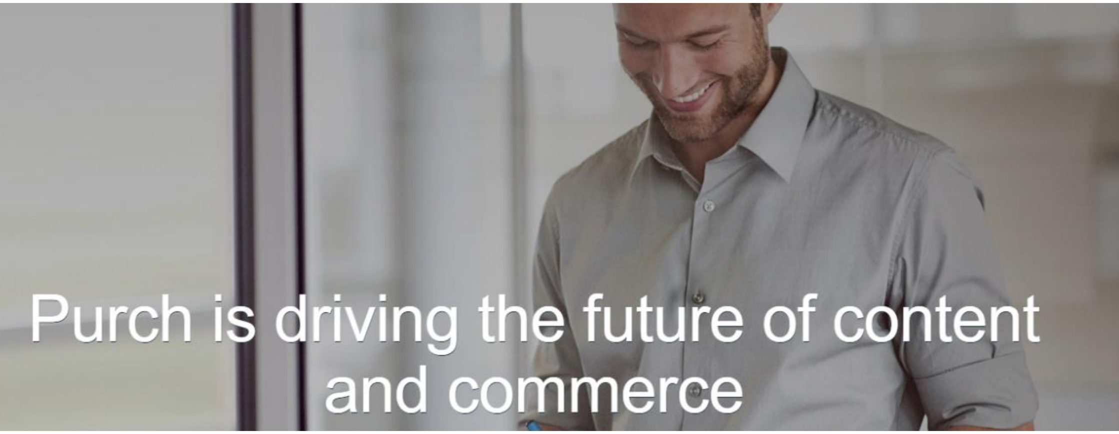
Moreover, it’s a great idea to integrate security concerns into hiring itself. When interviewing prospective employees, make sure this question is at the top of your mind: Is this person trustworthy?

4. Have policies in place

Probably the very best thing a business can do to keep its workplace safe is simply to have policies and procedures in place that address security needs. Don’t leave security up to individual judgment. Research best practices and enforce them across the board.

That way, when confronted with a potential threat, your staff will have a unified and stellar response to meet it with.

For many, security is an anxious topic. Many of us are so anxious at the thought of something going wrong that we’re afraid to adequately prepare. But equipped with these tips, it’s my hope that any business can make significant strides to ensure a safe, secure workplace.



We Are Purch

Purch is a rapidly growing, constantly evolving digital content and services company that helps millions of people make smarter purchases. We bring together 350 employees from around the globe who share a commitment to serve our customers with integrity, collaborate to deliver better results, and shape the future of digital publishing.

To view more content like this, visit **www.business.com**

To learn more about Purch, visit **www.purch.com/about**