Your

need-to-know guide to cloud security

Crosstek

Your need-to-know guide to cloud security

The growth of cloud computing has completely changed how we work. Zoom, Microsoft 365 – the whole array of collaboration tools that have become part of daily life over the past couple of years – these are all cloud-based applications that many of us wouldn't want to do without.

Storing data in the cloud has become standard for many businesses, thanks in part to its ability to grow as your business grows. You never pay for more storage than you need; you have access to more facilities than you would if you kept your data inhouse; and you have no need to maintain bulky servers.

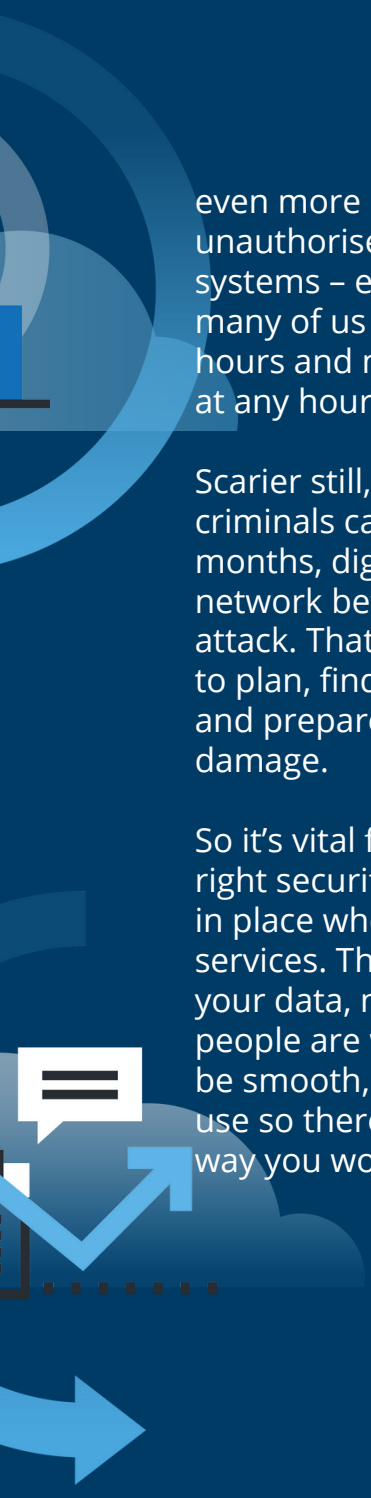
But security in a cloud environment can create challenges.

Cloud security encompasses all the policies, systems and services that protect your business from criminals. And since data is crucial to most businesses, protecting it should be taken seriously.

In the past, we mostly connected to our company networks from inside the office. That made it easier to protect the data within our own four walls. But we now access applications, documents, and services from anywhere, and that requires a very different approach to security.

In many ways, the move to the cloud has created an open invitation to cyber criminals. All they need to do is get hold of your login credentials and they're in – relatively simple phishing emails or brute force cyber-attacks are all it takes.

This provides the attacker with genuine credentials, making it



even more difficult to detect unauthorised access to your systems – especially now that many of us are working flexible hours and may access systems at any hour of the day or night.

Scarier still, once inside, cyber criminals can spend weeks, even months, digging around in your network before they launch an attack. That's to allow them time to plan, find your security flaws, and prepare to do the most damage.

So it's vital for you to have the right security tools and protocols in place when using cloud services. They should secure your data, no matter where your people are working from, but also be smooth, intuitive, and easy to use so there is no change in the way you work.

Cloud environments nearly always offer some security, but that doesn't mean they're not vulnerable to attack. They need to be correctly configured for security to be effective.

By mid-2021, almost 98% of businesses had experienced at least one security breach. The levels of crime are rising, and the number of affected businesses is growing...

Planning is key. That means keeping up with cloud security trends and being aware of the evolving challenges and threats.

In this essential guide, we look at the most effective ways to protect your cloud services. Some are simple to implement yourself, others may need more expertise. So buckle up for a few long words, and if you do feel that you need the support of a trusted IT expert, **just get in touch. It's what we do.**

Multi-Factor Authentication (MFA)

The most obvious way to keep your data protected is to introduce stronger security to your cloud login procedure. That's where MFA comes in. It's the equivalent of adding an electronic lock to the front door, and only giving the keycode to people with the right ID.

Multi-factor authentication requires a second-stage, single-use password to make the login process more secure. This second password is usually sent to a smartphone or generated via a secure USB key, so that only the intended person is able to use it.

According to Microsoft, MFA protects against 99.9% of fraudulent sign-in attempts.

The other good thing about MFA is that the second stage notification can act as an extra security alert. If, say, you receive a text with a single-use password, but you haven't attempted to log in to the application, you'll know that someone is trying to access your account. That allows you to take action to make sure they're not successful.

Use encryption

Storing, sharing and transferring data is a major benefit of cloud applications. But instead of taking these actions and thinking nothing of it, try adding encryption into the mix.

This means that your data is encoded the moment it leaves your device and stays that way in the cloud until you use it again, or share it with a privileged co-worker, for example. When it stays encrypted for the duration, this is called end-to-end encryption. It stops cyber criminals being able to hijack your data once it leaves your device or network. It also means that, should your cloud provider suffer a breach, any data that's stolen will be useless without a decryption key – which only you have.

Many cloud services will provide this service as part of your package. But it's good practice to make 100% sure, instead of assuming it's being done.

Cloud Security Posture Management

This isn't about taking care of your back. CSPM constantly monitors the services you use, which allows you to spot and fix security issues before they become a problem.

If you use one cloud service, chances are you use several of them, and keeping track of every app and server is a job in itself. Your data can be exposed if you inadvertently leave a cloud service open.

An expert IT service partner will be able to deploy CSPM monitoring for you across all your systems and applications.

Manage your user accounts

As with any of your sensitive data, you need to actively manage who is able to access what kinds of information.

Some members of your team, especially in IT, may have high-level admin accounts with full access to your entire system. As you may imagine, unauthorised access to this could be extremely detrimental. For that reason, admin-level devices should not be able to browse the web or read emails because of the increased risk if an account was compromised.

Make sure that employees who don't need admin access don't have it. The more people who have higher level access, the greater the opportunity for cyber criminals to gain entry to your cloud services.

Install the update

As with all applications, cloud services receive regular software updates to keep them working optimally, and to patch any new vulnerabilities.

It's important that these patches are applied immediately to prevent cyber criminals from taking advantage and entering your network.

Alerts are often issued about newly discovered vulnerabilities and it's important that you follow the alert's advice and apply any new updates.

Zero trust

The basic principle of zero trust is to never trust and always verify. That means you should always confirm the identity of anyone trying to access your cloud services, whether they are from within or outside of your network.

Zero trust also supports the 'least privilege' principle – that means that people are only given access to the things they need to perform their job, and nothing more.

Zero trust principles extend deep into the way chunks of data speak to each other in the cloud, so if you work with a lot of personal or business-critical information, you should definitely seek expert guidance on keeping it secure.

You still need to back up

You have a backup, right? Just because your data is in the cloud, it doesn't mean that you shouldn't be backing it up.

No network is impossible to breach. Your cloud security strategy – and indeed your entire security strategy – should always include storing offline backups of data. So if something happened that left your cloud services unavailable (like your provider suffering a major disaster of its own), your business wouldn't be thrown into chaos.

It also means that in the event of a ransomware attack, you still have all your data to work with. You do still have to worry about where stolen data could end up, but you can at least continue working.

Keep it simple

Cloud services should make things easier for everyone in a business, and your security should feel simple too.

Make sure you're using the right tools, that are effective, but also accessible and intuitive. If they're not, you risk your employees not using them at all.

If your processes are overcomplicated, employees will bypass security measures or save their work elsewhere – often within personal accounts – which is the complete opposite of security.

So for the best chance of keeping your cloud services secure, make tools easy to use and your rules simple to follow, to encourage people to work with them.

There's a lot to think about when it comes to the security of your cloud services. Some of these protections will already be offered by your cloud service provider, but if you're unsure, it's worth checking your set-up to understand if you could be at risk.

If you find that your cloud services aren't as secure as you'd like, or you simply don't know where to start, call on the experts.

That's us.

Get in touch today to find out what we can do to help keep your data more secure.

Crosstek

CALL: 01732 617788
EMAIL: jon.cross@crosstek.co.uk
WEBSITE: www.crosstek.co.uk