CLOUDCOCO
THE FUTURE STARTS NOW

The 7 Critical Control Points

Within any computer network there exists the risk of a security breach, compromise and loss. As cyber-attacks predominantly take place for financial gain, no business, however large or small is exempt from the threat. Whilst the risk cannot be avoided, all businesses need to ensure that systems are in place to mitigate the risks as much as possible.

There are several ways to do this, though many organisations, across many sectors, have wholly inadequate security in place that is not capable of preventing the increasingly complex threats that exist today.

The decision to deploy security measures also seems like a dark art, mystifying many of what is or isn't suitable, but CloudCoCo has a security framework that looks to remove the complexity and offer direction of where to begin and where to concentrate immediate effort.

Security protection has always been a layered approach as we need to build a Defence-in-Depth strategy to protect our data. Defence-in-Depth means that we have different ways of preventing the threat and that this should spread across a business's digital environment covering the Critical Control Points that are most likely to be targeted. These Critical Control Points are where businesses have the greatest risk of compromise and areas of weakness within these areas will inevitably increase the attack surface and the risk of a security incident.

The first Critical Control Point to protect is the **PERIMETER** of your environment, the figurative front door. Limiting what can have access is critical to not just blocking attacks but also limiting the reconnaissance that many cybercriminals will carry out before an attack takes place. Whilst many businesses have a firewall in place, the firewall should be able to inspect applications and have enhanced intrusion prevention capabilities. Your firewall should also feed into a reporting tool that can report on activity that is being blocked.

Due to Covid-19, many of us are working remotely, connecting back into our corporate systems from home using our residential internet connections. **REMOTE ACCESS** is therefore the second Critical Control Point that needs to be addressed. If you are allowing users access without security mechanisms in place you're leaving a window open where the front door can be bypassed. You must ensure that all users connect securely and are using multi-factor authentication as passwords alone are simply not sufficient.

The third Critical Control Point is the **DEVICE** which is used by the user. The traditional method of device protection, which is AntiVirus, is necessary but no longer sufficient on its own as a single protection layer since the effectiveness of the AntiVirus is dependant upon the speed at which a patch update can be issued and its effectiveness to block nuance changes. Additional device security, including Endpoint Detection and Sandboxing will add additional checks to verify the legitimacy of the files that the user can access.

Perhaps one of the most important Critical Control Points surrounds the **CLOUD STORAGE** of your data. As many businesses use many of the 100,000+ external cloud applications for either storage or transmission, we forget that once the data leaves our infrastructure it can no longer be controlled. A Cloud Storage policy, and more importantly how that is managed, is absolutely necessary to protect your data from being outside of your control. Once it leaves you'll never get it back!

The security risk that we are all familiar with is that of ransomware. With an increasing threat to the business, not just in loss of data but the disruption of loss of access to the data, a Critical Control

Point around **EMAIL** is essential. The vast majority of ransomware gets into our environments through email, and whilst we hope that our users will spot the dodgy email, increasingly complex spoof emails make that a risky strategy. Inspecting and blocking dangerous emails before they get to the users inbox is a necessary critical control point to have in place.

Knowing and limiting who has access to the local **NETWORK**, either through a physical cable or WIFI is, more often than not, the least thought about Critical Control Point that you have. As a rule, we're more open to giving WIFI access to visitors or leaving guest networks open without considering how access can spread beyond the confines of our buildings. Further, as users come back into the building having worked remotely with little or no security protection, we allow them to access the internal network bypassing all the controls we have in place. Our Networks need to be able to identify and quarantine users, whoever they are, that pose a threat to the network.

The final Critical Control Point is that of **INTERNET ACCESS**. Having restrictions to where users can browse to, whether by URL, category, application or content is essential to mitigating the risk of inadvertently allowing malicious content into the environment because a user has visited an inappropriate or infected website. Whilst some organisations leave Internet Access open to their users, certain categories, for the continued integrity and security of the data, need to be blocked.

These seven Critical Control Points are the absolute foundation of what needs to be in place as part of a business's cyber security protection framework and we would encourage a review of your current Defence-in-Depth strategy against these seven areas.

At CloudCoCo we believe that these Critical Control Points can be even more effective when the systems in place each interoperate and communicate to share intelligence. This is just one of the reasons why we highly recommend the Fortinet Security Fabric suite of solutions as the underlying platform to keep your data safe, not just from today's security threats, but also from tomorrow's.

If you would like to discuss your Critical Control Points and how CloudCoCo can assist with advising how to make your data much harder to lose, then we'd love to spend some time with you to discuss how minimal changes and additions can make a huge difference.

deg@cloudcoco.co.uk
03334559885
www.cloudcoco.co.uk