one brightly cyber

WE MAKE CYBER SIMPLE

ANOTHER CLOUD RISK

The benefits and risks of cloud service have been discussed in these Insights before. Here we will look at an aspect of securing the cloud environment that is not well-known.

Moving to the cloud is not as simple as moving some software and it magically works. The cloud environment and the virtual machines must be configured to meet each client's needs. Configuration responsibility is shared. Operating infrastructure belongs to the cloud provider and applications and data belong to the client. Both need to be properly configured for safety.

So far, so good. Now, it gets interesting. Your applications and data are on a virtual machine. How does that VM and applications interact with the cloud environment to get to real resources such as storage and network and more? The answer is software typically called middleware that facilitates the interaction.

The difficulty is that cloud providers have not always been upfront about the existence of this middleware, who created it, who installs it, who owns it, and who is responsible for keeping it up to date.

The middleware is typically more than one software package. To accommodate all possible levels of access between the two environments each piece of the middleware is typically given privileged access to make sure it has the access it needs to perform the functions. Privileged access at what is a machine-to-machine level is not unique to the cloud environment and has its counterparts in systems and applications running entirely in a company data center. However, the difference is if all is running in the client environment, then it is clear who chose it, who installed it, and who is responsible for it.

In the cloud environment the cloud vendor installs that software on the client's virtual machines, often without telling the client anything about it, such as whose software it is, or who is responsible for keeping it up to date. Or anything else.

Even if it is kept up to date, software often has vulnerabilities that aren't known until discovered by security investigators or cybercriminals.

The highest privileges may be necessary for their tasks, but my guess is that in many cases no one really looks at that. By assigning the highest privileges no one has to go back to increase privileges if tasks are added or changed that require them or if something fails. Don't think this software comes from unknown or small companies, or open source. It may come from them, but the major cloud vendors, Amazon, Google, and Microsoft may use their own software.

Regardless of the source of the software it may not be safe. For example, Microsoft Azure components used in this function have major vulnerabilities. One was recently discovered allowing a cybercriminal to gain root privileges. Root privileges allow the cybercriminal to go anywhere on the machine or virtual machine and install any other software they want. Chances are good that it will not benefit you.

WE MAKE CYBER SIMPLE

ANOTHER CLOUD RISK

Giving highest privilege goes against everything we have learned. Best practices say always assign the lowest level of privilege to a user that allows them to do their job. The rationale behind this is if the user gets hacked, the cybercriminals will have access to as little as possible.

Just because it is middleware or other machine to machine access doesn't make assigning full privileges any less risky. It may make things riskier because it allows moving between machines or virtual machines giving cybercriminals broader access to do damage.

What can you do? Insist upon a full list of all the software to be installed, sometimes called a Software Bill of Materials, SBOM. It needs to include every piece of software to be installed or used in the environment. Make sure you know who is responsible for installing it, who is responsible for maintaining it, and who is responsible for keeping it updated.

To help you discover the software typically installed by the major cloud vendors, a public database has been created by Wiz.io called The Cloud Middleware Dataset database project. Our mention of this is not an endorsement nor a recommendation nor a claim it is complete. We only reference it here as a courtesy.

Ultimately, the responsibility is yours. Insist that your cloud service provider provide an inventory of every piece of software they will install and who is responsible for it. Make sure that they are obligated to notify you if anything changes or is added after initial installation including new releases, and notification occurs in a timely manner.

Ask about the privileges given to these software modules and the justification for assigning that level of privilege.

Cloud services offer many benefits but in today's environment everything is fair game for cybercriminals. Not knowing what is in your cloud environment and who updates it is asking for trouble.

Ready to take the next steps? Contact onebrightlycyber at info@onebrightlycyber.com or call (888) 773-1920.