USER PRIVILEGES – A SIGNIFICANT RISK

Every user of company systems needs the proper privileges to access systems, applications and data.

To simplify the task and prevent frequent demands for access to additional resources IT often gives everyone access to everything.

Applications which need to access data in different places are also often given full privileges to access everything.

So, what is wrong with this approach? Everything! Giving everyone access to everything is just asking for trouble.

One way to think of access is like a hotel. When you check in you get a key card to open your room door, exercise center, business center, etc. But it won't open other guest rooms, administrative offices, conference rooms, the kitchen, storerooms, utility rooms, etc. where guests don't belong.

Remember 95% of cyber events are caused by people. Clicking a bad link or responding to a phishing email gives a cybercriminal your user credentials. And those credentials give access to everything, data, protected personal information for customers, patients, employees, everything.

If the attack was ransomware, all the servers and information on them will be encrypted. Probably information from them was downloaded by the cybercriminals before they were encrypted. How will your company function if every bit of information is not accessible? Whether you pay the ransom or attempt to use good backups, how long will it take to restore all the servers, all the databases, every bit of information? One week, two weeks, longer?

Will your company survive being out of business for that long? Will your customers have turned to your competitors?

Role-based access is a good answer to this dilemma. In role-based access each role within the company is defined. Then working with the manager of each role determine exactly which systems, applications and data are needed. And grant exactly that access and only that access.

Then when someone joins the firm or transfers to a new role, all IT needs is to know their role. That will provide the access they need. If something changes, it gets added to the list for that role. Then everyone with that role is automatically granted access to the new system, application, data, whatever.

And when someone leaves, their id is disabled and that removes access to everything they could access.

Role based access can't prevent a cyber incident, but in case of a compromise, it will limit what can be accessed.

And that is what you want - to protect company assets and legally protected information.

Want to learn more about cyber security and education, contact AIM Cyber at info@AIMglb.com or call (888) 773-1920.