Block People from Your Network that Have No Business Being There

Posted on May 01, Posted by Ira Greene Category Security

When a company is lax about their network security, this can lead to countless threats swarming the network and invading your systems. Yet, sometimes the most dangerous threats come from within. A common issue comes from employees accessing undisclosed files unintentionally and deleting them, which can cause more damage than you think.

Take, for instance, the food industry. There are several integral employees that a fast food restaurant employs. There are cashiers, managers, and food prep team members. The cashiers require access to the cash registers. The managers require access so they can count the drawers and record the day's profits. The average food prep employee, though, doesn't need to access the cash drawers. Therefore, they have no reason to do so.

This is how the principle of least privilege operates. It's the act of limiting access to crucial assets in an attempt to expose them to the least amount of potential threats. This includes making sure that users only access files that are absolutely required for their position. This entails setting up additional security features that limit which user accesses what files. Depending on the solution, it could be anything from a simple process, like user filtering, to an external program or piece of hardware which restricts access to certain information.

Limiting user privileges on workstations is also a common best practice in the industry. For example, the average user doesn't need to run programs with administrator privileges in order to function properly. Instead, reserve these rights for only those who need to do so, like your management staff and your internal IT department.

The main reason to limit access to particular data isn't because you don't trust your employees. It's more about restricting access and mitigating risk factors than anything else. The fewer users who have permission to view the confidential data, the lower the chance that security discrepancies can arise. It should be mentioned, however, that no security measure can keep all threats at bay. This is why it's important to practice maximum caution and take preventative measures to limit the damage that can be done by hacking attacks.

Lighthouse Technology Solutions has the ability to restrict access to certain parts of your network on a user basis. We can monitor and maintain your network for any suspicious activity, as well as take detailed audits of login attempts, network traffic, and more.

More often than not, even a comprehensive solution like this isn't enough to keep your business's network secure. Even with minimal user permissions, threats have a way of worming themselves into your infrastructure when you least expect them to. One way to augment our monitoring services is with our Unified Threat Management (UTM) solution. This consists of most everything your business's network security could ask for, including a firewall, enterprise-level antivirus, spam blocking, and content filtering services. You'll be sure that you have the best security measures put in place for your business.

For more information and best practices concerning network security, give Lighthouse Technology Solutions a call at 703-533-LTSI (5874).

Tags: Tagged in: Customer Relationship Management Network Phone System Security

User

VoIP