cloudIT

Beware of your employees!

https://cloudit.co

Beware of your employees!

If someone asked you what was the biggest threat to your business from the IT perspective, what would come to your mind first? Data loss, natural disasters, server crashes, hacking, etc., right? Wrong! Studies show that one of the biggest reasons businesses end up becoming a victim of cybercrime is their own employees. This whitepaper tells you how it works and what you can do to prevent it from happening.

Employees often unwittingly 'help' cyber criminals gain access to your system

We are not saying that your employees are malicious, just that, too often, employees play a part in compromising the security of your IT infrastructure, even without realizing it. Some such scenarios include-

BYOD environment

The Bring Your Own Device (BYOD) trend, while great at bringing flexibility to your work zone, also brings a lot of risk to the table. BYOD means your employees use their own devices for work purposes as well--to access emails, to connect to work servers and even to work on office files. So, if their device ever gets infected by a malware or hacked, the virus or the hacker gets access to your data as well. Plus, you cannot control how your employees use their personal devices. They may connect to unauthorized networks, download unauthorized software, use outdated antivirus programs etc,. Even something as simple and harmless as the free Wi-Fi at the mall can spell danger for your data. In the BYOD environment, losing personal devices such as smartphones, laptops or tablets is like opening the virtual floodgates to all kind of malwares and phishing attacks.

Inability to differentiate between genuine and malicious messages

Your employees may fall victim to phishing messages and scams and expose your network to the biggest risks out there unintentionally. Clicking on a fake link that looks genuine or sending sensitive information to a fake email ID that impersonates the original one are just disasters waiting to happen.

Finally, there may be a few of those employees whose moral compass doesn't exactly point north. Disgruntled employees looking to make a few quick bucks may actually compromise confidential business data intentionally.

So, what can you do to keep your IT safe?

Train your employees

Train your employees so they don't end up sabotaging your IT infrastructure accidentally. Conduct drills, workshops and training sessions that help them identify spam, malware, malicious links, messages and files. Follow up with tests to ensure they really understand what you shared and take it seriously.

Strong BYOD policies

The BYOD scenario is great, but not establishing rules and boundaries related to it is not. Establish clear policies in relation to BYOD. For example, employees using their own devices for work purpose should turn in their devices for monthly/quarterly audits, have firewalls installed, system updates done, antivirus updated, etc

Passwords

Password leaks by employees are a commonplace. Easy passwords can be hacked, shared passwords can be misused. To avoid an IT disaster as a result of a password leak or hack, make sure you have a password policy in place. Teach your employees the best practices of password creation and management. Conduct timely audits to ensure the passwords match the specified safety standards and password management in your written your policy. Also, take corrective actions against employees who don't follow your password policies related to password sharing, setting, etc.

That takes care of the unintentional security breaches, what about the malicious ones? Monitor

Finally, there may be a few of those employees whose moral compass doesn't exactly point north. Disgruntled employees looking to make a few quick bucks may actually compromise on confidential business data intentionally.

It is great to trust your employees, but it is also important to monitor their work activities to identify any abnormalities. There are two components to this--one is physical and the other is virtual. On the physical side, we have systems like CCTVs, biometric access, etc., whereas on the virtual side, we have software programs that track employee activities when they are accessing your network and data. Such software provides you with screenshots of your employee's work device screen when they are logged onto the system, alert you upon certain activities such as plugging in an external device like a hard disk or pendrive or data copying or even access of data at hours that are 'odd' in comparison to the general trend. For example, an employee accessing data on weekends or at the dead of the night or on holiday can trigger an alarm.

IT is the lifeblood of your business and when you let your employees access your IT network, you are, in a way, trusting them with your business. Make sure they are trained and trustworthy enough.

CONTACT DETAILS

cloudIT

Mel Cook
vCIO | Cloud IT, LLC
mcook@cloudit.co
Phone: 513.347.4343
https://cloudit.co