Armor Security & The Internet of Things (IOT) Safety

The internet is a tool that can be used to bring business or stop business.

Technology is continually advancing. Along with this is the continual need for security, data back up and peace of mind. As I have grown my business into Armor, focusing on I.T. Services and Electronic Repair, we have continued to have to increase our security and anticipate failure. There are 5 main concerns for your home and business that you need to focus on.

1. Have a good firewall.
2. Practice good internet habits and have a good virus scanner.
3. Have a duplicate set of your critical data stored offsite and check it.
4. Do not rely on your phone or computer.
5. If you can afford it, pay for redundancy in everything.

ONE – Having a good firewall in your network will help you control everything from the computers themselves to the people attacking your systems. Armor had has been involved in massive Distributed Denial of Service (DDOS) Attacks. This is where a single or group of systems access the

Written by David A Galica, Armor Technologies – 9/11/2017

Armor is a group of people lead by David A. Galica. The focus of Armor is developing solutions using opensource software and designing systems to ensure the education of the staff and success of the clients. Armor's goals are not to outsource an economy that can be local. To understand the technology, we develop I.T.

network and continually send packets of data at the server or firewall to drain the bandwidth so it is unreachable by the rest of the world. When we were attacked we had more than 1 Gigabit of data drained from the bandwidth that making it appear that our server was down along with the entire city of Rochelle Illinois. The firewall in Rochelle was not accessible to us and RMU that hosted us would just turn us off. We migrated our server to DeKalb and the attacked followed our host name.

The firewall in Dekalb that we controlled could collect all the IP address of the attacking systems. However, we did not have enough bandwidth to operate. Ultimately, we moved all our clients out to another host we resell for. This ended us as the only local hosting company in the area. However, the firewall gave us the IP addresses to begin scanning at tracking what turned out to be a paid attack by a bot net through an IRC Chat Channel. We have been scanning over 1000 infected systems across the globe. The most common systems we come across are Windows XP and Windows 7 machines with out of date virus scanners.

Our firewall know notifies us of any issues, by rule sets, that may be causing problems and will black list people immediately. We currently recommend a custom firewall with PFSense installed. Contact Armor for more information.

TWO – Practicing good internet habits and having a good virus scan will typically save your systems. Do not open emails that have nothing to do with you. Hover over links to show the real location and make an educated judgement call before

clicking. If you are unsure about something being a scam, call your local I.T. company or a friend that knows. It is ok to be cautious. LinkedIn, Yahoo, ARP, even Equifax has been hacked and millions of people's accounts have been comprised. You can be cautious.

On your mobile devices, you need to read the fine print on the apps you install. You give access to most of your information with most apps. It is best to not save passwords on your mobile devices unless you are keeping it limited to only the apps you use regularly.

Have a good virus scanner. Even a MAC can get a virus. A virus scanner working with the computers firewall will stop most threats. They have a piece of software that has definitions of viruses and an algorithm to guess strings that perform malicious functions. Those algorithms are called heuristics. Most virus scanners are rated by those. Some virus scanners do have data mining software that reports what you do on your computer to the company. We do not recommend any software that does data mining.

Practice those good habits and have a good virus scanner. We recommend using a combination of Malwarebytes and Avira or GData products. Contact Armor for more information.

THREE – Have a duplicate set of data on a second secure system is key to keep running after critical failure. A business has a 100% chance of critical failure in any system with mechanical parts and people operating them. Hard drives fail, data, files, pictures, and the numbers you need can be lost. Small computers, and servers can have

redundant drives but another part can still fail. There are a few simple ways to stay up. 1. A usb flash drive or back up drive can be used to make a copy and set aside. 2. Offsite network backup solutions can be used to back up your data in the cloud. 3. Fully mirrored servers for 100% redundancy can be implemented for a high price tag. 1 and 2 are typically the most common methods and all you must do is get yourself into a schedule to check them.

Don't forget what data is important. Most people leave out their internet short cuts and their address book from their Outlook or other email client. Also try to consolidate your data into one location for easy back up.

We have worked for a 100 Million Dollar company that their ERP system had failed loosing 4 months of operations. It cost the company 10s of thousands of dollars in rebuilding that data plus loss of productivity. Even though a backup was in place, it was not checked frequently. The SQL database was not copying correctly on the automated backup. Another company had been backing up their data to a flash drive and left it in the computer when the building burned down. They lost a month of data. It was still costly to a small business.

We have seen the loss of wedding photos, children's first pictures, QuickBooks files, years of research, because the backup was not checked. We recommend a combination of a computer with redundant hard drives and an encrypted online backup solution that you log in to periodically to

check that it is working. Contact Armor for more information.

FOUR – Do not rely on your phone or computer. This is your technology disaster recovery plan. I know this sounds odd, but if you have all your data in a second location then just in case your computer or phone goes down then you can just get on another one.

How many times does your internet go down a year? How many times does your phone system go down? How long does your website go down? Your communications can be set up on other devices. You can go and set up a Gmail account and a google phone number with all your address book and phone book to get right back up while rebuilding your systems.

Armor builds I.T.s own.

Our website, email, phone system, and servers went up and down for 10 days. We had other computers we communicated by social media. We had other cell phones to communicate with clients. We made it through the problems by using other devices and communication systems.

We recommend a pbx based phone system that can roll over to a cell phone. We recommend having a secondary email system such as Gmail to communicate with clients. We recommend utilizing a home office back up system to get to files you need to continue to operate. Remote software can be set up to allow retrieval of data. Contact Armor for more information.

FIVE – If you can afford it, pay for redundancy in everything. It sounds expensive. However, if you can manage your budget and use technology to

automate systems you can save the money you would have lost. Build two of the same systems. Have one back up to the other daily, weekly, or monthly. If one goes down then use the other. While technology is continually getting less expensive the software is increasing in cost due to the complexity of systems that is backing up and managing. Some costs are going down by paying monthly fees.

Each computer or server that is built can run multiple systems in VMware or Virtual Box systems. Consolidating the software per system will make an easier back up set.

While Armor had one main Web server we always have spare parts and multiple internet connections for redundancy. Now we have even more redundant connections after the DDOS attacks that we have sustained. We are also moving more data to more systems. We have multiple devices running multiple connections to give us minimal down time and access from any location. It is costly. However, if we had this before we could have shortened our 10 days up and down to 1 day up and down.

We recommend 2 mirror systems with virtualized software to push closer to 100% reliability. Contact Armor for more information.

Armor Technologies

143 E Lincoln Hwy

DeKalb IL 60115

www.ArmorTechs.com

(815) 754-0505