MILE Technologies Inc.

The approach to security best practices

BY LOUIS LOPEZ

There is no such thing as security. There is only a balance of the sense of security, the risk, and the complexity.

- LOUIS LOPEZ – MILE TECHNOLOGIES, INC.

Security points

- Everyone is vulnerable. Because they are vulnerable, the security of the systems they use is vulnerable
- The system is any component involved in IT that allows access to obtaining data
- Physical security is only as secure as the levels required to touch it.
- Passwords that are not stored and have another layer of required verification are best
- Key cards can be less secure because they can be obtained
- Biometrics can be less secure because they can be obtained
- Passwords without verification can be less secure because they can be intercepted
- Untrained users are the vulnerability of all of these securities
- Backups and recovery access and speeds are key to continuation of business flow
- The lower the security, the quicker the data can be accessed or compromised

The best approach is basic.
Begin security – Close the front door.

- Use a supported and updated Operating System
- Use a supported and updated Antivirus
- Perform your Windows updates automated
- Perform your Antivirus updates automated
- Add layers of physical security to be able to access your IT system
- Add a local backup to fast backups and recovery
- Check the local backups to make sure they are working
- Add a backup to the cloud
- Check the cloud backups to make sure they are working
- Train yourself and the users of the IT system for basics
- Update the training regularly to educate the weak spots, the users.
- You cannot secure your home until you close the front door

Layers of security

Advanced security – Add a lock, deadbolt, monitored alarm, insurance.

- Add bitlocker on Windows Professional
- Deploy a content filter to the IT system
- Add antispam to your email system
- Roll out antimalware software
- Add self-updating firewalls
- Update policies as necessary
- Lock-down workstations with strict policies
- Create a disaster recovery policy
- Write a retirement of hardware policy
- Create an security incident report policy
- Add authenticator verifications to all online accounts
- Deny any mix of personal equipment into business applications

Security insanity and paranoia

Red level security – 1000ft of concrete block on all sides of IT and unplugged

- Orange level security is the closest level of real secure (more that the others)
- Require all of the following
- UEFI secure boot
- BIOS Boot password
- Bitlocker boot password and USB Key
- Login password with key-fab login
- MFA authenticators for all access
- Zero access to all and allow access only to required
- Dedicated hardware per person
- Auditing on all access
- Encrypted data access using software like fasoo. Data cannot be accessed even if it is taken outside IT system.
- Red level security can be achieved if it is unplugged, turned off, drained of all power, and physically inaccessible

MILE Technologies Inc.

The approach to security best practices

BY LOUIS LOPEZ