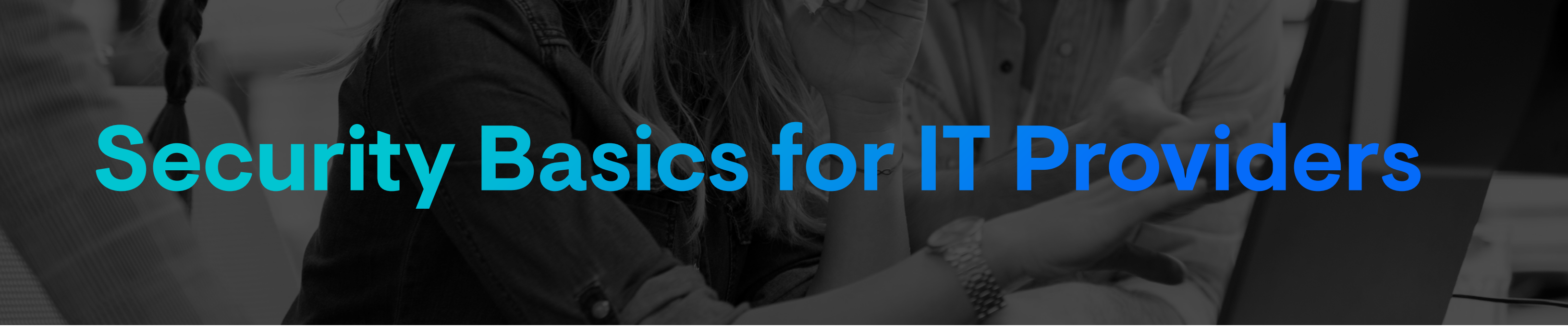


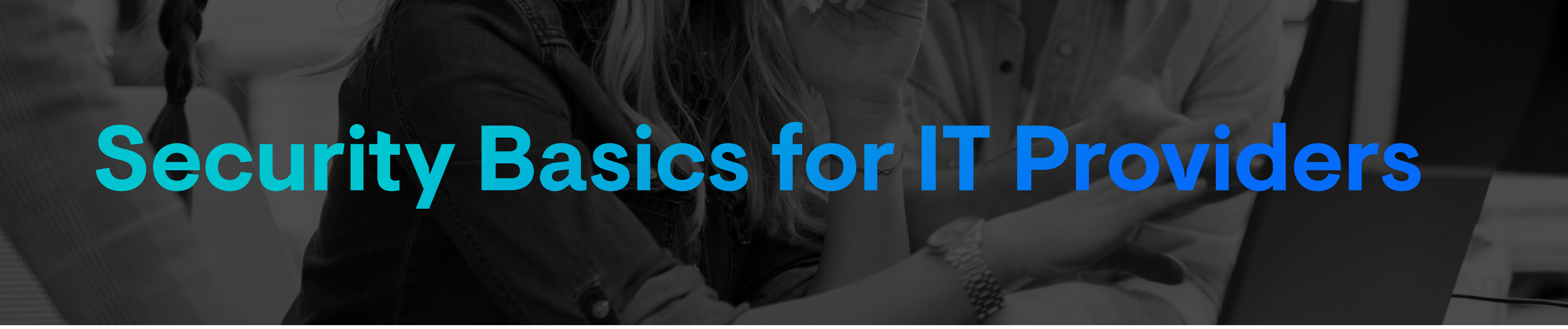
Security Basics for IT Providers

SECURITY BASICS CHECKLIST FOR IT PROVIDERS

Threat actors love to find and exploit low-hanging fruit. Make their job harder by following these cybersecurity basics for IT providers.

- □ **Get your baseline identified and document everything.**
  - □ Make sure you document everything with a network address
    - □ Identify those switches without IPs
  - □ Document software and versions
  - □ Identify unsupported OS
  - □ Identify and document data access control lists
  - □ Identify and document privileged accounts
  - □ Identify and document externally available ports
    - □ Close threat-producing ports like RDP, SMB, SSH (both external and internal)
  - □ Document and confirm all security controls are in place and working
    - □ Firewall IDS
    - □ Endpoint protections
    - □ Spam filtering solutions
- □ **Patch it all. (Timely patching is key.)**
  - □ Hardware
  - □ Hypervisors
  - □ 3rd party software
    - □ Monitor security resources like cve.mitre.org for information about key CVEs
- □ **Enable multi-factor authentication (MFA) on everything.**
  - □ Priority 1: All internal systems
  - □ Priority 2: All customer systems
    - □ Focus first on their email
      Business email compromise (BEC) is still the number one money-making activity for threat actors
    - □ Remote access tools like VPN

* Disclaimer: Any actions taken need to be tailored to your unique situation and environment. We don't take responsibility for results or outcomes.



Security Basics for IT Providers

- □ **Implement a cybersecurity training program for both new and existing employees.**
  - □ Require new employees to complete training as part of their onboarding
  - □ Implement regular interactive trainings that engage end users
- □ **Establish least privilege access.**
  - □ Remove local admin rights
    - □ If a person needs admin rights, create a second login with a different passphrase (or use privileged access management [PAM] software)
- □ **Ensure data access is correctly restricted.**
- □ **Enforce the usage of a password management solution.**
  - □ Configure complex passphrases (15 character minimum)
  - □ Require unique passphrases for everything
  - □ Set up auto-locking of machines
- □ **Implement a backup solution that is offsite and segregated from the environment.**
- □ **Configure your remote monitoring and management (RMM) software.**
  - □ Reinstall key security software or restart services
  - □ Enforce logging and save at least 7 days of information
    - □ Write to disk if necessary
  - □ Alert on privileged account creation
- □ **Encrypt your data.**
  - □ Ensure all workstations have BitLocker and store keys in Active Directory
    - □ Export to another location periodically in case Active Directory is down
  - □ Configure email encryption

* Disclaimer: Any actions taken need to be tailored to your unique situation and environment. We don't take responsibility for results or outcomes.