US SIGNAL®

CYBERSECURITY CHECKLIST

FOR MSPs

Cybercriminals don't restrict themselves to targeting the big, rich companies. They've discovered that MPSs and other vendors to these companies can be just as lucrative of targets. That's because they can make money off these third-party companies, and often access their business customers as well — but only if the initial targets aren't prepared.

The following list can help with that preparation. While it's not comprehensive and the specifics will vary by company, it provides a starting point for shoring up security to keep cybercriminals out and preventing them from moving on to your customers should they get in.

Restrict Network Access

- [ ] Enable multi-factor authentication whenever possible.
- [ ] Avoid using default usernames such as admin, administrator, default, and user.
- [ ] Limit privileges to the minimum required to perform necessary functions.
- [ ] Create buffers between different tiers of privileged access.
- [ ] Block lateral movement between workstations.

Secure Remote Management Tools

- [ ] Keep remote management software up to date.
- [ ] Enable centralized logging/monitoring and alerting for remote access sessions.
- [ ] Restrict access to remote management tools and accounts.
- [ ] Limit what remote accounts can access.
- [ ] Don't log into workstations with domain administrator accounts.

Assess Remote Desktop (RDP/RDS) Systems

- [ ] Identify systems that have been compromised with RDP backdoors.
- [ ] Disable RDP on devices that don't need it.
- [ ] Implement an account lockout policy to prevent successful brute-force attacks.
- [ ] Log off disconnected and idle sessions.
- [ ] Leave Network Level Authentication (NLA) enabled.

Protect Users and Endpoints

- [ ] Keep endpoint systems and software current by automating patch management.
- [ ] Use DNS filtering to protect against known malicious websites.
- [ ] Use spam filtering for active email protection.
- [ ] Provide frequent security awareness training to employees to help them spot malicious emails and websites.
- [ ] Use a reliable backup solution with multiple restore points as well as offsite replication.

Review Monitoring Tools and Technologies

- [ ] Use RMM and/or SIEM to configure centralized network and endpoint monitoring.
- [ ] Create standard monitoring and alert settings you can apply across devices.
- [ ] Prioritize alerts based on severity and create notification policies for each.
- [ ] Use an endpoint detection and response (EDR) solution.
- [ ] Determine if you need to outsource management of all or some of the above to a managed detection and response (MDR) provider.

Implement an Incident Response Plan

- [ ] Identify various types of security incidents.
- [ ] Establish roles, responsibilities, and procedures for responding to these incidents.
- [ ] Identify escalation options in case an incident requires more expertise than you have available.
- [ ] Plan for communicating internally, with customers, authorities, and the public.
- [ ] Know your organization's compliance requirements regarding incident disclosure and reporting.

Educate Customers

- [ ] Share security best practices with your customers.
- [ ] Provide recommendations for must-have security tools and technologies, such as endpoint detection and response (EDR) and next-gen firewalls.
- [ ] Impress upon your customers the importance of backup/disaster recovery.
- [ ] If you have the capabilities, offer vulnerability management services and security assessments (or suggest companies that can provide them.)
- [ ] Create a culture of security with your customers.

Partner for Better IT Security

The best IT security strategy is one in which all parties – service providers, customers and all third-party companies – work together. For more information and services to make this happen, contact US Signal.