KPMG

Remote Workforce - Managing Cyber Risk

Are you confident your remote workforce is protected from cyber threats?

1. Why remote workforce risk assessments are a necessity for businesses

Companies have been shifting to more flexible and dynamic workplace structures over the past few years and this has been even more accelerated by recent events leading to remote and distributed working infrastructure.

With these changes are increased risks because connectivity and data flow in new ways which traditional infrastructure may not be prepared to protect.

Organizations cannot afford to have their business disrupted by cyber attacks allowed by these new environments. Leading organizations are taking action to establish confidence that their remote workforces have a secure and resilient infrastructure in place to run their business.

2. Organizations are shifting to remote workforce models all over the world

BYOD and Mobile Devices
Employees access company data from mobile phones and personal computers with web email access

Cloud Applications
IT is decentralized and not restricted to one physical on premise datacenter

VPN Connections
The company network is spread out and connected across remote sites

3. Many organizations struggle to secure increased remote infrastructure

1. **Unsecured Remote Wifi connections**
2. **Unapproved cloud file sharing tools**
3. **Work email access on personal devices**
4. **Cloud system remote administrative access**
5. **Meeting conference software vulnerabilities**
6. **Lack of physical access protection**

4. Organizations are facing the impact and implications of the risk

- **Business outages and downtime due to cyber attack**
- **Regulatory penalties and fines for negligence of data security**
- **Loss of customer confidence in brand and reputation**
- **Intellectual property losses of sensitive information to competitors**

Checklist - Remote Work Cyber Controls

Technology	Cyber Control
Remote Computer Endpoints	1. Are your remote endpoints checked for vulnerable configurations and outdated patches frequently? 2. Can the security team detect if remote endpoints are compromised and respond accordingly? 3. Do your remote endpoints require multifactor authentication to access your company network and servers? 4. Is privileged access from remote endpoints limited to only those who need it and only while needed?
Mobile Endpoints	5. Are mobile devices centrally managed to enforce passcodes, device encryption, OS updates, and remote wipe capabilities?
Remote Access Servers **On-Prem & Cloud**	6. Is there an inventory of the different methods to remotely access your internal and cloud systems (ie. VPN Tunneling, Application Clients, Portals, Remote Desktop Services)? 7. Architecture – Have the internal systems and devices which provision remote access been placed on the perimeter network such as the DMZ with restricted access to the internal network? 8. Are remote access servers checked for vulnerable configurations and outdated patches frequently? 9. Can the security team detect if the remote access servers are compromised and remotely respond to the incident? 10. Is privileged access to remote access servers internally and in the cloud limited to only those who need it and only while they need it? 11. Do the remote access servers require mutual authentication so that the endpoint confirms the server identity before providing credentials? 12. Do the remote servers require strong network encryption (ie. TLS 1.2)?
Emails	13. Do you have an email gateway in place which filters malicious emails and alerts the security team of suspicious behavior? 14. Is web browser access to email either disabled or required to use multifactor authentication? 15. Are users made aware how to detect and report phishing emails?
Web Browsing	16. Do you have a web gateway in place for all web browsing from company devices which filters malicious websites and alerts the security team of suspicious behavior?
External File Sharing	17. Do users know to only use approved external file sharing or cloud storage solutions? 18. Is there monitoring in place to detect the use of unauthorized external file sharing or cloud storage solutions from company computers?
Video Conference	19. Do users know to only use approved video conferencing tools? 20. Does the approved video conferencing tool use secure configurations (ie. require a password, use waiting room, disable recording)
Confidential Data	21. Do users know what data is confidential and how that data should be stored and shared?

Contact Us:

Manav Prakash
Partner, *Advisory*
KPMG Fakhro
E: mprakash@kpmg.com

Logan Simpson
Head of Cyber Security Services
KPMG Fakhro
E: jlsimpson@kpmg.com