

BEST CYBER SECURITY PRACTICES

IN THIS PANDEMIC SITUATION

FACTS AND FIGURES

775%

Microsoft's cloud services reported a 775% increase in demand across their platforms when strict social isolation measures were put in place.
-Microsoft Officials

Increased independence on Digital tools has led to hacker's target.

209 Days

In 2019, the average time it took businesses to detect a data breach was close to 7 months. Organizations meanwhile needed an average of 73 days to contain a breach.
- All About Security

\$133.7 billion

Global cybersecurity spending is expected to reach \$133.7 billion by 2022
-RSAConference

\$3.92M

Data Breaches cost enterprises an average of \$3.92 Million and 27% are due to human errors
- Security Intelligence Data Breach Report 2019

39 sec

The malicious hacking attack occurs every 39 sec.
- University of Maryland

94%

94% of malware is delivered via email.
-CSO

1. Endpoint Security compliance check

- Ensure **continuous detection** and monitoring mechanisms are in place and functioning
- Organizations should have the ability to manage their endpoints and check its **compliance** while users are not connected to the corporate networks
- Bring your own device (BYOD) policies are defined and **security** checks in place for scanning the systems for policy checks before permitting to connect.

2. Data Security and Privacy a Priority

- Employees having access to confidential data or PI data should be trained on the emphasis of confidentiality and **secure handling of data**
- Such employees access should be governed periodically and ensure least privilege policy is maintained
- Adequate training to the employees on company policies and awareness program. Educating them on various techniques like phishing and more used for exploits
- Engage solutions which could identify possible data leakages like source code leak, credentials leak

3. User awareness training programs

- Interactive training sessions to engage users in understanding organizations infosec policies and good practices to be followed
- Simulated attack-based training has proven effective in educating users, so it is a good option for organizations to adopt such training for users
- Such training should also include good practices to be adopted by users while working from home

4. Multi-Factor Authentication for Protection

- MFA has become one of the key factors for two-step verification and secures personal information with special controls with VPNs
- MFA should also be extended to some critical applications/systems adding another layer of protection
- Ensure the device authorization check is included as part of your VPN connectivity

5. Privilege User Management

- Privilege accounts are the most critical components of **access management**, and there has to be processed in place to check if RBAC is aligned on the principle of least privilege
- In this situation, it suggested to increase the frequency of privilege account audits and clean up immediately upon identification

6. Vulnerability Assessment and Patch Management.

- Identify critical service components like VPN gateways, critical services contributing to remote access and increase the frequency of scanning and patching
- Ensure regular **vulnerability assessment** process is more governed and adopt prioritization based on risk for the organization rather just on the risk scores of the vulnerability
- Ensure end-user machines connected remotely are being governed through corporate **patch management** solution.

7. Practice Cyber-Hygiene Habits

- Educate users to avoid usage of the public network and instead invest in a dependable private network for internet access and preferably through corporate VPN.
- Ensure corporate VPN/Remote access gateways are properly configured as per defined corporate policies and are being patched regularly.
- Keep anti-virus definition and system patching up to date

8. Process Report Incident

- Reporting any security issues to the IT Team
- Educate users on what all qualifies as a security incident and importance of reporting any security issues to the IT Team
- Outlook plugin will be an added advantage to report suspicious emails.
- Ask the security monitoring teams to keep a close look on active threats and campaigns triggered to exploit the COVID situation

9. Using Secure means of Communication

- Any interaction related to work need to be communicated through secure means of communication or Security enabled tools
- Do not use freeware for any video conferencing or data sharing related to corporate information exchange.

About Happiest Minds Technologies

Happiest Minds, the Mindful IT Company, applies agile methodologies to enable digital transformation for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights. We leverage a spectrum of disruptive technologies such as: Big Data Analytics, AI & Cognitive Computing, Internet of Things, Cloud, Security, SDN-NFV, Blockchain, Automation including RPA, etc. Positioned as "Born Digital . Born Agile", our capabilities spans across product engineering, digital business solutions, infrastructure management and security services. We deliver these services across industry sectors such as retail, consumer packaged goods, edutech, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/transportation/hospitality.

A Great Place to Work-Certified™ company, Happiest Minds is headquartered in Bangalore, India with operations in the U.S., UK, The Netherlands, Australia and Middle East.

Write to us at
Business@happiestminds.com