

9

tips for protecting your organization from cyberattacks



HAVE A PLAN

Think about how you will maintain business continuity. Have the necessary contacts at hand and prepare a plan for starting recovery.



EMPOWER YOUR PEOPLE

People on the IT floor know what your organization lacks. They just need approval and resources to handle it. You can use DevOps to help manage the process.



CONSIDER THE HUMAN COST

Security protects not just your data, but also the people at your organization. Think of the pressure an attack might put them under, and the long-term economic impact.



MAKE SECURITY EVERYONE'S BUSINESS

You can't do it alone. Build an understanding of security and educate your people. Engage with, listen to, and trust them to help you identify and patch up the weak spots

5

STEPS TO PROTECT USERS AND THEIR IDENTITIES

Start with these simple yet often overlooked tasks:

- Enable MFA
- Prevent the use of simple passwords
- Do not share privileges between work and administrative accounts
- Patch your systems
- Use dedicated admin workstations



SET UP PROPER ACCESS PRIVILEGES

Implement a Tiered Access Model for your AD and Azure AD environment. It doesn't require new tools or licenses. You don't have to apply it to all accounts, just the ones that need it.



KNOW YOUR ENVIRONMENT

You need to know what business-critical applications you have on board. Gather and analyze logs, and use SIEM services like Azure Sentinel to help you spot the threats and mitigate them



USE SUPPORTING TOOLS

You can purchase tools which will give you even more possibilities to protect your organization from threats. Try tools for advanced threat protection, like Defender ATP

and remember...

THIS IS ABOUT YOU!

No organization is immune to a cyber threat. If there's value in your data and IT systems, your business is a target. Make sure you're prepared!