www.ibs.com.cy

AZURE ACTIVE DIRECTORY: PROTECT YOUR BUSINESS WITH A UNIVERSAL IDENTITY PLATFORM

By Achilleas Eleftheriou – Technical Manager

What is Azure Active Directory?

Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service, which provides Single Sign-On (SSO) and Multifactor authentication to help protect your users from 99.9% of cybersecurity attacks, in addition helps your employees sing in and access resources in:

- **External resources** - such as Azure portal, O365, and thousands of other Software as a Service (SaaS) applications.
- **Internal resources** - like apps on your corporate network and intranet along with any cloud apps developed by your own organization.

In 2020 unfortunately we came across Covid-19, one virus that has altered the way we work and socialize. Now that physical distancing has become essential to protect everyone's health, more people than ever are going online to connect and get things done.
So, in these challenging times Azure AD can make life simpler, both for people working from home and for IT Administrators charged with keeping their infrastructures secure.

The following are top five recommendations for empowering remote work:

1. **Use a common collaboration tool** (like Microsoft Teams, Cisco Webex, Slack, Workplace by Facebook, Zoom)
2. **Enable your users to securely access cloud apps from outside your corporate network**
   To ensure your association, it's important that when you empower access to cloud applications from individual gadgets and remote areas, it is done safely. In case you're now utilizing Azure AD Conditional Access, you realize very well that may be utilized to apply security approaches to help guarantee the correct individuals approach the applications they need, in accordance with your hierarchical prerequisites. You can stretch out your strategies

to ensure all your applications, requiring controls like passing an MFA challenge or utilizing an agreeable gadget.

3. **Provide secure access to your on-premises infrastructure from outside your company network**

   Most companies are running lots of business-critical applications on-premises, many of which may not be accessible from outside the company network. Azure AD Application Proxy is a lightweight agent that enables internet access to your on-premises apps, without opening broad access to your network.

4. **Collaborate with your partners**

   With many companies cancelling non-essential business travel, working closely with business partners can become more difficult. Azure AD's B2B collaboration capabilities can help you use your chosen collaboration app—including SharePoint, Teams, and Google Drive—securely across company boundaries.

5. **Support bring-your-own-device**

   Not every organization can provide corporate devices for remote work, but you can enable access to company data on personally owned devices using Microsoft Intune app protection policies combined with Azure AD Conditional Access.

Achilleas Eleftheriou is working with IBSCY LTD for the last 7 years. During his employment with IBSCY, he had several roles starting from junior positions. Currently, he is our Technical Manager. His background is mostly on networking, but he has also vast experience on systems implementations with Windows Server, local and in the cloud. He is the head of our technical implementations team and holds a BSc in Computer Science from Frederick University plus several certifications from FortiNet and Microsoft.