Securing Cloud PCs and Azure Virtual Desktop : Start Implementing and Optimizing Security for Windows 365 and AVD Infrastructure

Verham, Dominiek

Monografía

Enhance your security expertise in Microsoft virtual desktops by exploring the latest security controls and use cases to safeguard your Windows 365 and Azure Virtual Desktop infrastructure Key Features Understand the importance of securing your endpoints and overcome security challenges Learn about the latest Microsoft security controls for Windows 365 and AVD Gain an understanding of securing virtual environments through various use cases Purchase of the print or Kindle book includes a free PDF eBook Book Description Do you want to effectively implement and maintain secure virtualized systems? This book will give you a comprehensive understanding of Microsoft virtual endpoints, from the fundamentals of Windows 365 and Azure Virtual Desktop to advanced security measures, enabling you to secure, manage, and optimize virtualized environments in line with contemporary cybersecurity challenges. You'll start with an introduction to Microsoft technologies, gaining a foundational understanding of their capabilities. Next, you'll delve into the importance of endpoint security, addressing the challenges faced by companies in safeguarding their digital perimeters. This book serves as a practical guide to securing virtual endpoints, covering topics such as network access, data leakage prevention, update management, threat detection, and access control configuration. As you progress, the book offers insights into the nuanced security measures required for Windows 365, Azure Virtual Desktop, and the broader Microsoft Azure infrastructure. The book concludes with real-world use cases, providing practical scenarios for deploying Windows 365 and Azure Virtual Desktop. By the end of this book, you'll be equipped with practical skills for implementing and evaluating robust endpoint security strategies. What you will learn Become familiar with Windows 365 and Microsoft Azure Virtual Desktop as a solution Uncover the security implications when company data is stored on an endpoint Understand the security implications of multiple users on an endpoint Get up to speed with network security and identity controls Find out how to prevent data leakage on the endpoint Understand various patching strategies and implementations Discover when and how to use Windows 365 through use cases Explore when and how to use Azure Virtual Desktop through use cases Who this book is for This book caters to a diverse audience within the IT landscape. For IT directors and decision makers, it provides valuable insights into the security benefits of implementing virtual desktops, emphasizing the contribution to a more secure environment. IT consultants and engineers will find practical tools and guidance for securely managing Microsoft cloud-based virtual desktops. Security professionals will benefit from the expert knowledge and alignment with industry best practices, while students can deepen their understanding of securing AVD and W365

Título: Securing Cloud PCs and Azure Virtual Desktop Start Implementing and Optimizing Security for Windows 365 and AVD Infrastructure

Edición: 1st ed

Editorial: Birmingham Packt Publishing, Limited 2024 2024

Descripción física: 1 online resource (396 pages)

Contenido: Cover -- Title page -- Copyright and credits -- Foreword 1 -- Foreword 2 -- Contributors -- Table of Contents -- Preface -- Part 1: An Introduction to Microsoft Virtual Desktops -- Chapter 1: Introducing Windows 365 and Azure Virtual Desktop -- Advantages of using a virtual desktop -- Introducing Windows 365 -- Features of Windows 365 -- Windows 365 editions -- Introducing Azure Virtual Desktop -- Licensing Windows 365 and Azure Virtual Desktop -- Licensing Windows 365 -- Licensing Azure Virtual Desktop -- Introducing Windows App -- Summary -- Part 2: Why Is Endpoint Security Important? -- Chapter 2: Importance of Securing Your Desktops -- A desktop at the heart of a user's workspace -- Multiple users on a single desktop -- What happens when a physical desktop is lost or stolen? -- What can IT admins do to prevent data leakage? -- What about the Remote lock device action? -- Summary -- Chapter 3: Modern Security Risks -- What are bad actors? -- Types of cyberattacks -- Phishing attack -- Ransomware -- Distributed denial of service -- Man in the middle attacks -- SQL injections -- Cross-site scripting -- Zero-day exploits -- Social engineering attacks -- Recovering from a cyberattack -- A cyber incident response plan -- Virtual desktops to the rescue -- Summary -- Part 3: Security Controls for W365 and AVD -- Chapter 4: Securing User Sessions -- CA and MFA -- Security defaults -- Per-user MFA -- CA policy -- Configuring RDP device and resource redirections for Windows 365 -- Device and resource redirections with Intune -- Device and resource redirections with group policy -- Configuring RDP properties for Azure Virtual Desktop -- Drive and storage redirection -- Clipboard redirection -- COM port redirection -- Printer redirection -- Smartcard redirection -- USB device redirection -- RDP session limit timeouts -- Summary Chapter 5: Preventing Data Leakage from Desktops -- Preventing screen captures -- Enabling screen capture protection for Windows 365 -- Enabling screen capture protection for Azure Virtual Desktop -- Introducing and configuring watermarking -- Enabling watermarking for Windows 365 -- Resolving information in QR codes -- Enabling watermarking for Azure Virtual Desktop -- Configuring screen locks -- Dynamic locking -- Screen savers -- Smart cards -- Session time limits -- Summary -- Chapter 6: Update Management Strategies -- Windows Update for Business -- Windows Autopatch -- Licensing Windows Autopatch -- Enrolling into Windows Autopatch -- Registering devices to Windows Autopatch -- Release management in Windows Autopatch -- Autopatch groups -- Managing the Windows Autopatch service -- Managing updates using custom image templates -- Introducing custom image templates -- Preparing for custom image templates -- Creating a custom image template -- Using custom image templates as part of the update strategy -- Manually creating custom images -- The prerequisites to creating a custom image -- Creating a custom image for Windows 365 -- Creating a custom image for Azure Virtual Desktop -- Summary -- Chapter 7: Threat Detection and Prevention -- Microsoft Defender for Endpoint -- Requirements for Microsoft Defender for Endpoint -- Enrolling Windows 365 Cloud PCs into Microsoft Defender for Endpoint -- Using a security baseline as a starting point -- Enrolling an Azure Virtual Desktop session host into Microsoft Defender for Endpoint -- Introducing tamper protection -- Enabling tamper protection -- Verifying the tamper protection status -- Tamper-protected settings -- Encrypting data on the virtual desktop -- Encryption for Windows 365 Cloud PCs -- Encryption for Azure Virtual Desktop session hosts -- Summary -- Chapter 8: Configuring Access Control Configuring Role-Based Access Control (RBAC) -- RBAC for AVD -- Management group RBAC assignment -- Subscription RBAC assignment -- Resource group RBAC assignment -- RBAC for Windows 365 -- Azure Bastion -- Azure Bastion custom role -- Using Azure Bastion -- Configuring JIT -- Microsoft Privileged Identity Management -- Windows Local Administrator Password Solution (LAPS) -- Windows LAPS Azure Virtual Desktop -- Windows LAPS for Cloud PCs -- Summary -- Part 4: Additional Security Controls per Solution -- Chapter 9: Securing Windows 365 -- Introducing the Windows 365 advanced deployment guide -- Deployment options -- Pre-deployment options -- Security guidelines for Windows 365 -- Local admin rights -- Endpoint Privilege Management -- Creating an elevation settings policy -- Creating an elevation rules policy -- Acquiring the file hash -- Creating and exporting Cloud PC restore points -- Creating a restore point -- Exporting a restore point --

Placing a Cloud PC under review -- Tips and tricks -- Tip 1 - Use Windows 365 Boot with multiple Cloud PCs -- Tip 2 - Make sure that users always have to sign in to the Cloud PC -- Summary -- Chapter 10: Securing Azure Virtual Desktop -- Configuring backups -- Creating a Recovery Services vault -- Backup policy session hosts -- Restoring session hosts -- Backup policy for FSLogix -- Restoring an FSLogix profile -- Securing AVD with private endpoints -- Host pool private endpoints -- Workspace private endpoints -- Trusted launch and confidential computing -- Trusted launch -- Confidential computing -- Configuring AppLocker -- Securing OneDrive -- Securing OneDrive with a GPO -- Securing OneDrive with Intune -- Active Directory structure and security -- Separated OU -- Separated GPO for each environment -- Dedicated service account to domain join -- Summary -- Chapter 11: Securing Azure Infrastructure Configure storage security -- RBAC roles on the storage account -- Applying the correct NTFS permissions -- Configuring private access using a private endpoint -- Configuring NSGs -- Configure network security with Azure Firewall -- Using IP groups in firewall policies -- Configure network security with NSGs -- Deploying AVD on dedicated hosts -- Configuring Defender for Cloud -- Deploying an Azure VPN gateway -- Summary -- Part 5: Use Cases -- Chapter 12: Windows 365 Use Cases -- When to use Windows 365 as your personal desktop -- Windows 365 as a replacement for on-premise VDI -- Why is Windows 365 a good alternative to an on-premise VDI? -- Windows 365 for contractors -- Why is Windows 365 a good solution to provide a secure desktop for contractors? -- Using Windows 365 as a privileged access workstation -- Why is Windows 365 a good solution as a PAW? -- How Windows 365 Boot helps to secure an endpoint -- Why is using Windows 365 Boot a good way to secure a local desktop? -- Enhancing security by restricting access to Office 365 services to Cloud PCs -- The scenario of restricting Office 365 access to Cloud PCs -- How to restrict Office 365 access to Cloud PCs -- Windows 365 Frontline versus Windows 365 Enterprise -- Why should companies prefer Frontline Cloud PCs? -- How to license for Windows 365 Frontline -- Summary -- Chapter 13: Azure Virtual Desktop Use Cases -- AVD for external users using Bring Your Own Device (BYOD) -- Using remote apps instead of desktops -- AVD as a disaster recovery solution -- AVD for a break/fix scenario -- Running AVD on Azure Stack HCI -- Summary -- Index -- Other Books You May Enjoy

ISBN: 1-83546-114-X

Materia Título preferido: Microsoft Office- Security measures

Materia: Virtual computer systems- Security measures Informática en la nube- Security measures Computer security Microsoft Azure (Computing platform)- Security measures

Autores: Vanneuville, Johan Brinkhoff, Christiaan Manchester, Scott

Enlace a formato físico adicional: 1-83546-025-9

Baratz Innovación Documental

- Gran Vía, 59 28013 Madrid
- (+34) 91 456 03 60
- informa@baratz.es