1. Record Nr. UNINA9911019850003321

Autore	Hughes Chris
Titolo	Effective Vulnerability Management : Managing Risk in the Vulnerable Digital Ecosystem
Pubbl/distr/stampa	Newark : , : John Wiley & Sons, Incorporated, , 2024 ©2024
ISBN	1-394-22122-3 1-394-27715-6
Edizione	[1st ed.]
Descrizione fisica	1 online resource (291 pages)
Altri autori (Persone)	RobinsonNikki
Disciplina	005.8
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Cover -- Title Page -- Copyright Page -- Contents at a Glance -- Contents -- Foreword -- Introduction -- What Does This Book Cover? -- Who Should Read This Book -- How to Contact the Publisher -- How to Contact the Authors -- Chapter 1 Asset Management -- Physical and Mobile Asset Management -- Consumer IoT Assets -- Software Assets -- Cloud Asset Management -- Multicloud Environments -- Hybrid Cloud Environments -- Third-Party Software and Open Source Software (OSS) -- Third-Party Software (and Risk) -- Accounting for Open Source Software -- On-Premises and Cloud Asset Inventories -- On-Premises Data Centers -- Tooling -- Asset Management Tools -- Vulnerability Scanning Tools -- Cloud Inventory Management Tools -- Ephemeral Assets -- Sources of Truth -- Asset Management Risk -- Log4j -- Missing and Unaccounted-for Assets -- Unknown Unknowns -- Patch Management -- Recommendations for Asset Management -- Asset Manager Responsibilities -- Asset Discovery -- Getting the Right Tooling -- Digital Transformation -- Establishing and Decommissioning Standard Operating Procedures -- Summary -- Chapter 2 Patch Management -- Foundations of Patch Management -- Manual Patch Management -- Risks of Manual Patching -- Manual Patching Tooling -- Automated Patch Management -- Benefits of Automated vs. Manual Patching -- Combination of Manual and Automated Patching -- Risks of Automated Patching -- Patch

Management for Development Environments -- Open Source Patching -- Not All Software Is Equal -- Managing OSS Patches Internally -- Responsibilities of Infrastructure vs. Operations Teams -- Who Owns Patch Management? -- Separation of Duties -- Tools and Reporting -- Patching Outdated Systems -- End-of-Life Software -- Unpatched Open Source Software -- Residual Risk -- Common Attacks for Unpatched Systems -- Prioritizing Patching Activities.
Risk Management and Patching -- Building a Patch Management Program -- People -- Process -- Technology -- Summary -- Chapter 3 Secure Configuration -- Regulations, Frameworks, and Laws -- NSA and CISA Top Ten Cybersecurity Misconfigurations -- Default Configurations of Software and Applications -- Improper Separation of User/Administrator Privilege -- Insufficient Internal Network Monitoring -- Lack of Network Segmentation -- Poor Patch Management -- Bypass of System Access Controls -- Weak or Misconfigured Multifactor Authentication Methods -- Lack of Phishing-Resistant MFA -- Insufficient Access Control Lists on Network Shares and Services -- Poor Credential Hygiene -- Unrestricted Code Execution -- Mitigations -- Default Configurations of Software Applications -- Improper Separation of User/Administration Privilege -- Insufficient Network Monitoring -- Poor Patch Management -- Wrapping up the CIS Misconfigurations Guidance -- CIS Benchmarks -- DISA Security Technical Implementation Guides -- Summary -- Chapter 4 Continuous Vulnerability Management -- CIS Control 7-Continuous Vulnerability Management -- Establish and Maintain a Vulnerability Management Process -- Establish and Maintain a Remediation Process -- Perform Automated Operating System Patch Management -- Perform Automated Application Patch Management -- Perform Automated Vulnerability Scans of Internal Enterprise Assets -- Perform Automated Vulnerability Scans of Externally Exposed Enterprise Assets -- Remediate Detected Vulnerabilities -- Continuous Monitoring Practices -- Summary -- Chapter 5 Vulnerability Scoring and Software Identification -- Common Vulnerability Scoring System -- CVSS 4.0 at a Glance -- Base Metrics -- Exploitability Metrics -- Threat Metrics -- Environmental Metrics -- Supplemental Metrics -- Qualitative Severity Rating Scale -- Vector String.
Exploit Prediction Scoring System -- EPSS 3.0-Prioritizing Through Prediction -- EPSS 3.0 -- Moving Forward -- Stakeholder-Specific Vulnerability Categorization -- CISA SSVC Guide -- Decision Tree Example -- Software Identification Formats -- Common Platform Enumeration -- Package URL -- Software Identification Tags -- Common Weaknesses and Enumerations -- Summary -- Chapter 6 Vulnerability and Exploit Database Management -- National Vulnerability Database (NVD) -- Sonatype Open Source Software Index -- Open Source Vulnerabilities -- GitHub Advisory Database -- Exploit Databases -- Exploit-DB -- Metasploit -- GitHub -- Summary -- Chapter 7 Vulnerability Chaining -- Vulnerability Chaining Attacks -- Exploit Chains -- Daisy Chains -- Vendor-Released Chains -- Microsoft Active Directory -- VMware vRealize Products -- iPhone Exploit Chain -- Vulnerability Chaining and Scoring -- Common Vulnerability Scoring System -- EPSS -- Gaps in the Industry -- Vulnerability Chaining Blindness -- Terminology -- Usage in Vulnerability Management Programs -- The Human Aspect of Vulnerability Chaining -- Phishing -- Business Email Compromise -- Social Engineering -- Integration into VMPs -- Leadership Principles -- Security Practitioner Integration -- IT and Development Usage -- Summary -- Chapter 8 Vulnerability Threat Intelligence -- Why Is Threat Intel Important to VMPs? -- Where to Start -- Technical Threat

Intelligence -- Tactical Threat Intelligence -- Strategic Threat Intelligence -- Operational Threat Intelligence -- Threat Hunting -- Integrating Threat Intel into VMPs -- People -- Process -- Technology -- Summary -- Chapter 9 Cloud, DevSecOps, and Software Supply Chain Security -- Cloud Service Models and Shared Responsibility -- Hybrid and Multicloud Environments -- Containers -- Kubernetes -- Serverless -- DevSecOps -- Open Source Software. Software-as-a-Service -- Systemic Risks -- Summary -- Chapter 10 The Human Element in Vulnerability Management -- Human Factors Engineering -- Human Factors Security Engineering -- Context Switching -- Vulnerability Dashboards -- Vulnerability Reports -- Cognition and Metacognition -- Vulnerability Cognition -- The Art of Decision-Making -- Decision Fatigue -- Alert Fatigue -- Volume of Vulnerabilities Released -- Required Patches and Configurations -- Vulnerability Management Fatigue -- Mental Workload -- Integration of Human Factors into a VMP -- Start Small -- Consider a Consultant -- Summary -- Chapter 11 Secure-by-Design -- Secure-by-Design/Default -- Secure-by-Design -- Secure-by-Default -- Software Product Security Principles -- Principle 1: Take Ownership of Customer Security Outcomes -- Principle 2: Embrace Radical Transparency and Accountability -- Principle 3: Lead from the Top -- Secure-by-Design Tactics -- Secure-by-Default Tactics -- Hardening vs. Loosening Guides -- Recommendations for Customers -- Threat Modeling -- Secure Software Development -- SSDF Details -- Prepare the Organization (PO) -- Protect Software (PS) -- Produce Well-Secured Software (PW) -- Respond to Vulnerabilities (RV) -- Security Chaos Engineering and Resilience -- Summary -- Chapter 12 Vulnerability Management Maturity Model -- Step 1: Asset Management -- Step 2: Secure Configuration -- Step 3: Continuous Monitoring -- Step 4: Automated Vulnerability Management -- Step 5: Integrating Human Factors -- Step 6: Vulnerability Threat Intelligence -- Summary -- Acknowledgments -- About the Authors -- About the Technical Editor -- Index -- EULA.

Sommario/riassunto

Infuse efficiency into risk mitigation practices by optimizing resource use with the latest best practices in vulnerability management Organizations spend tremendous time and resources addressing vulnerabilities to their technology, software, and organizations. But are those time and resources well spent? Often, the answer is no, because we rely on outdated practices and inefficient, scattershot approaches. Effective Vulnerability Management takes a fresh look at a core component of cybersecurity, revealing the practices, processes, and tools that can enable today's organizations to mitigate risk efficiently and expediently in the era of Cloud, DevSecOps and Zero Trust. Every organization now relies on third-party software and services, ever-changing cloud technologies, and business practices that introduce tremendous potential for risk, requiring constant vigilance. It's more crucial than ever for organizations to successfully minimize the risk to the rest of the organization's success. This book describes the assessment, planning, monitoring, and resource allocation tasks each company must undertake for successful vulnerability management. And it enables readers to do away with unnecessary steps, streamlining the process of securing organizational data and operations. It also covers key emerging domains such as software supply chain security and human factors in cybersecurity. * Learn the important difference between asset management, patch management, and vulnerability management and how they need to function cohesively * Build a real-time understanding of risk through secure configuration and continuous monitoring * Implement best practices like vulnerability

scoring, prioritization and design interactions to reduce risks from human psychology and behaviors * Discover new types of attacks like vulnerability chaining, and find out how to secure your assets against them Effective Vulnerability Management is a new and essential volume for executives, risk program leaders, engineers, systems administrators, and anyone involved in managing systems and software in our modern digitally-driven society.