



Wieso, weshalb, warum: IT-Security?!

Ein exemplarischer Überblick über die von Wien Digital gesetzten Maßnahmen zum Schutz ihrer (Geo-)Service-Infrastruktur



Inhalt

- Vorstellung
- IT-Security – Ein Überblick
- Schutzmaßnahmen von Wien Digital
- Fragen & Antworten

Wer bin ich?

Wer bin ich?

- Marco Ender, marco.ender@wien.gv.at
- MA 01 – Wien Digital
 - Team Security & Safety
 - WienCERT – **C**omputer **E**mergency **R**esponse **T**eam
 - Security Engineering & Vorgaben
 - Technische Audits & Penetration Testing
 - Incident Response
 - Kooperation mit anderen CERTs

Woher komme ich – die IT von Wien Digital in Zahlen

- Hardware
 - ca. 10.000 Server, davon 72% virtualisiert
 - ca. 86.000 Arbeitsplatz-Endgeräte (PCs, Notebooks, ThinClients)
 - ca. 26.000 Drucker und Multifunktionsgeräte
 - ca. 62.500 Telefonanschlüsse
- Storage / Datenbanken
 - ca. 21.000 TB Storage
 - ca. 5.300 Datenbanken

IT-Security – ein Überblick

IT-Security – Wieso eigentlich?



IT-Security – Wieso eigentlich?

THE ECONOMIC TIMES | tech

English Edition | Today's ePaper

Home ETPrime Markets News Industry Rise Politics Wealth Mutual Funds Tech Careers

Web Stories Information Tech (IT) Tech & Internet Funding Startups Tech Bytes Newsletters Blog

Business News > Tech > Tech & Internet > ICMR data leak reveals personal info of 81.5 cr Indians, claims report; CBI likely to probe

ICMR data leak reveals personal info of 81.5 cr Indians, claims report; CBI likely to probe the breach

Mirror Now | 31 Oct 2023, 11:08 PM IST



BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

BLAME CLOP —

Mass exploitation of critical MOVEit flaw is ransacking orgs big and small

SQL injection attacks on MOVEit file-transfer service likely to get worse.

DAN GOODIN - 6/6/2023, 5:05 AM



Wieso, weshalb, warum: IT-Security?! [Frei verfügbar]

Exploitation of Citrix Zero-Day by Possible Espionage Actors (CVE-2023-3519)

JAMES NUGENT, FOTI CASTELAN, DOUG BIENSTOCK, JUSTIN MOORE, JOSH MURCHIE

JUL 21, 2023 | 10 MIN READ | LAST UPDATED: JUL 25, 2023

heise online > Microsoft > M

Microsofts gestohlener Schlüssel mächtiger als vermutet

Ein gestohlener Schlüssel funktionierte möglicherweise nicht nur bei Exchange Online, sondern war eine Art Masterkey für große Teile der Microsoft-Cloud.

YOUR FILES
ARE ENCRYPTED
BY LOCKBIT



What happens?

Many of your documents, databases, videos and other important files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our



How to recover my files?

We guarantee that you can recover all your files safely and easily. You can decrypt a single file for warranty - we can do it. But if you want to decrypt all your files, you need to pay.

haveibeenpwned.com/PwnedWebsites#WienerBuechereien



Wiener Büchereien

In June 2019, the library of Vienna (Wiener Büchereien) included 224k unique email addresses, names, physical addresses. The breached data was subsequently posted to Twitter by the

Breach date: 10 June 2019

Date added to HIBP: 28 June 2019

Compromised accounts: 224,119

Compromised data: Dates of birth, Email addresses, Names

Permalink

IT-Security – Und was schützen wir?

- Security schützt Assets
In der IT: Daten, Programme, IT-Systeme, Infrastruktur
In Folge aber auch z.B. Menschen (OT/NISG!)
- Confidentiality – Vertraulichkeit
- Integrity – Integrität
- Availability – Verfügbarkeit



Preservation of confidentiality, integrity and availability of information. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved. – ISO 27001

IT-Security – Und wovor schützen wir die IT?

- Vor Personen, Technik, Naturgewalten
- Sowohl absichtliche als auch unabsichtliche Verletzung der Schutzziele
- Angreifer
 - Skript Kiddies 🧪👍
 - Hacker (Whitehats 🛠️ vs. Blackhats 💰)
 - Kriminelle (Cryptolocker) 💰
 - Spionage (Wirtschaft / Militär / Nachrichtendienste) 💰 🕵️
- Verärgerte / ehemalige / bestochene / erpresste MitarbeiterInnen



IT-Security – Was tun Angreifer denn so?

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 17 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (5)	Abuse Elevation Control Mechanism (5)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (3)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Client Software Binary	Create or Modify System Process (4)	Deploy Container	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Create Account (3)	Create or Modify System Policy Modification (2)	Direct Volume Access	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Endpoint Denial of Service (4)
Search Open Technical Databases (3)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (4)	Domain Policy Modification (2)	Domain Policy Modification (2)	Modify Authentication Process (8)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Exfiltration Over Web Service (4)	Financial Theft
Search Open Websites/Domains (3)	Trusted Relationship	Trusted Relationship	Serverless Execution	Event Triggered Execution (16)	Escape to Host	Execution Guardrails (1)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Ingress Tool Transfer	Exfiltration Over Web Service (4)	Firmware Corruption
Search Victim-Owned Websites	Shared Modules	Valid Accounts (4)	External Remote Services	Event Triggered Execution (16)	Exploitation for Defense Evasion	Exploitation for Defense Evasion	Multi-Factor Authentication Request Generation	Device Driver Discovery	File and Directory Discovery	Data from Local System	Multi-Stage Channels	Scheduled Transfer	Inhibit System Recovery
	Software Deployment Tools		Hijack Execution Flow (12)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)	File and Directory Permissions Modification (2)	Network Sniffing	Domain Trust Discovery	Group Policy Discovery	Data from Network Shared Drive	Non-Application Layer Protocol	Transfer Data to Cloud Account	Network Denial of Service (2)
	System Services (2)		Implant Internal Image	Hijack Execution Flow (12)	Hide Artifacts (11)	Hide Artifacts (11)	Network Service Discovery	File and Directory Discovery	Log Enumeration	Data from Removable Media	Non-Standard Port		Resource Hijacking
	User Execution (3)		Modify Authentication Process (8)	Process Injection (12)	Hijack Execution Flow (12)	Hijack Execution Flow (12)	Network Share Discovery	Group Policy Discovery	Network Service Discovery	Data from Staged (2)	Protocol Tunneling		Service Stop
	Windows Management Instrumentation		Office Application Startup (6)	Scheduled Task/Job (5)	Impair Defenses (11)	Impair Defenses (11)	Network Sniffing	Device Driver Discovery	Network Sniffing	Email Collection (3)	Remote Access Software		System Shutdown/Reboot
			Power Settings	Valid Accounts (4)	Indicator Removal (9)	Indicator Removal (9)	OS Credential Dumping (8)	Domain Trust Discovery	Network Sniffing	Input Capture (4)	Traffic Signaling (2)		
			Pre-OS Boot (5)		Indirect Command Execution	Indirect Command Execution	Steal Application Access Token	File and Directory Discovery	Password Policy Discovery	Screen Capture	Web Service (3)		
			Scheduled Task/Job (5)		Masquerading (9)	Masquerading (9)	Steal or Forge Authentication Certificates	Group Policy Discovery	Peripheral Device Discovery	Video Capture			
			Server Software Component (5)		Modify Authentication Process (8)	Modify Authentication Process (8)	Steal or Forge Kerberos Tickets (4)	Log Enumeration	Permission Groups Discovery (3)				
			Traffic Signaling (2)		Modify Cloud Compute Infrastructure (5)	Modify Cloud Compute Infrastructure (5)	Steal Web Session Cookie	Log Enumeration	Process Discovery				
			Valid Accounts (4)		Modify Registry	Modify Registry	Unsecured Credentials (8)	Log Enumeration	Query Registry				
					Modify System Image (2)	Modify System Image (2)		Log Enumeration	Remote System Discovery				
					Network Boundary Bridging (1)	Network Boundary Bridging (1)		Log Enumeration	Software Discovery (1)				
					Obfuscated Files or Information (12)	Obfuscated Files or Information (12)		Log Enumeration	System Information Discovery				
					Plist File Modification	Plist File Modification		Log Enumeration	System Location Discovery (1)				
					Pre-OS Boot (5)	Pre-OS Boot (5)		Log Enumeration	System Network Configuration Discovery (2)				
					Process Injection (12)	Process Injection (12)		Log Enumeration	System Network Connections Discovery				
					Reflective Code Loading	Reflective Code Loading		Log Enumeration	System Owner/User Discovery				
					Rogue Domain Controller	Rogue Domain Controller		Log Enumeration	System Service Discovery				
					Rootkit	Rootkit		Log Enumeration	System Time Discovery				
					Subvert Trust Controls (6)	Subvert Trust Controls (6)		Log Enumeration	Virtualization/Sandbox Evasion (3)				
					System Binary Proxy Execution (13)	System Binary Proxy Execution (13)		Log Enumeration					
					System Script Proxy Execution (1)	System Script Proxy Execution (1)		Log Enumeration					
					Template Injection	Template Injection		Log Enumeration					
					Traffic Signaling (2)	Traffic Signaling (2)		Log Enumeration					
					Trusted Developer Utilities Proxy Execution (1)	Trusted Developer Utilities Proxy Execution (1)		Log Enumeration					
					Unused/Unsupported Cloud	Unused/Unsupported Cloud		Log Enumeration					

IT-Security – Was tun Angreifer denn so?

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (5)	Abuse Elevation Control Mechanism (5)
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Access Token Manipulation (5)	BITS Jobs
Gather Victim Network Information (6)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Account Manipulation (6)	Build Image on Host
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Autostart Execution (14)	Debugger Evasion
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Client Software Binary	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information
Search Closed Sources (2)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Create Account (3)	Create or Modify System Process (4)	Deploy Container
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (4)	Domain Policy Modification (2)	Direct Volume Access
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (16)	Domain Policy Modification (2)	Execution Guardrails (1)
Search Victim-Owned ...		Valid Accounts (4)	Shared Modules		Escape to Host	Exploitation for Defense Evasion
					Event Triggered	File and Directory

IT-Security – Was tun Angreifer denn so?

Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 17 techniques	Exfiltration 9 techniques	Impact 14 techniques
Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Endpoint Denial of Service (4)
Modify Authentication Process (8)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels		Financial Theft
Multi-Factor Authentication	Debugger Evasion		Data from Information Repositories (3)	Ingress Tool Transfer		Firmware Corruption
	Device Driver Discovery		Data from Local			Inhibit System Recovery
	Domain Trust Discovery					Network Denial of Service (2)
	File and Directory Discovery					

Schutzmaßnahmen von Wien Digital

Schutzmaßnahmen – Versuch einer Kategorisierung

- Controls == Maßnahme, Steuerung
- Controls nach Bereich
 - Administrative
 - Physical
 - Technical
- Controls nach Zielsetzung
 - Preventive
 - Detective
 - Corrective

Fragen & Antworten



Danke

