Wieso, weshalb, warum: IT-Security?!

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

Stadt Wien | Wien Digital

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 Career

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

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.

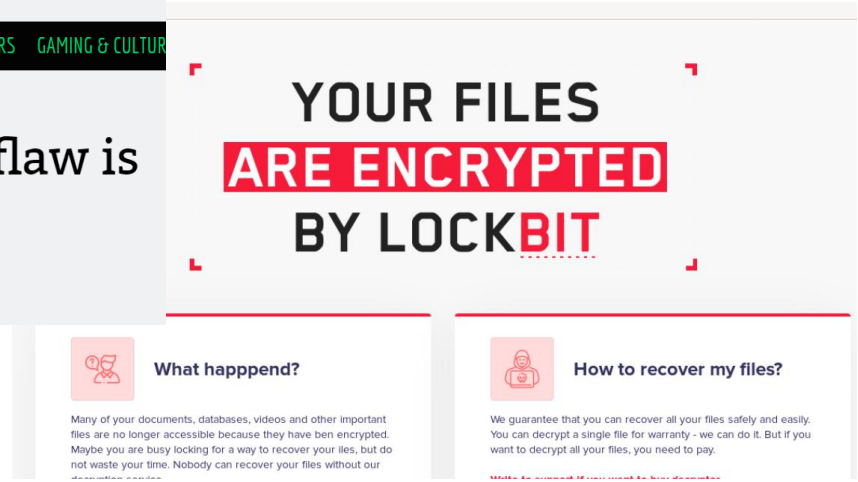
ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTUR

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



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

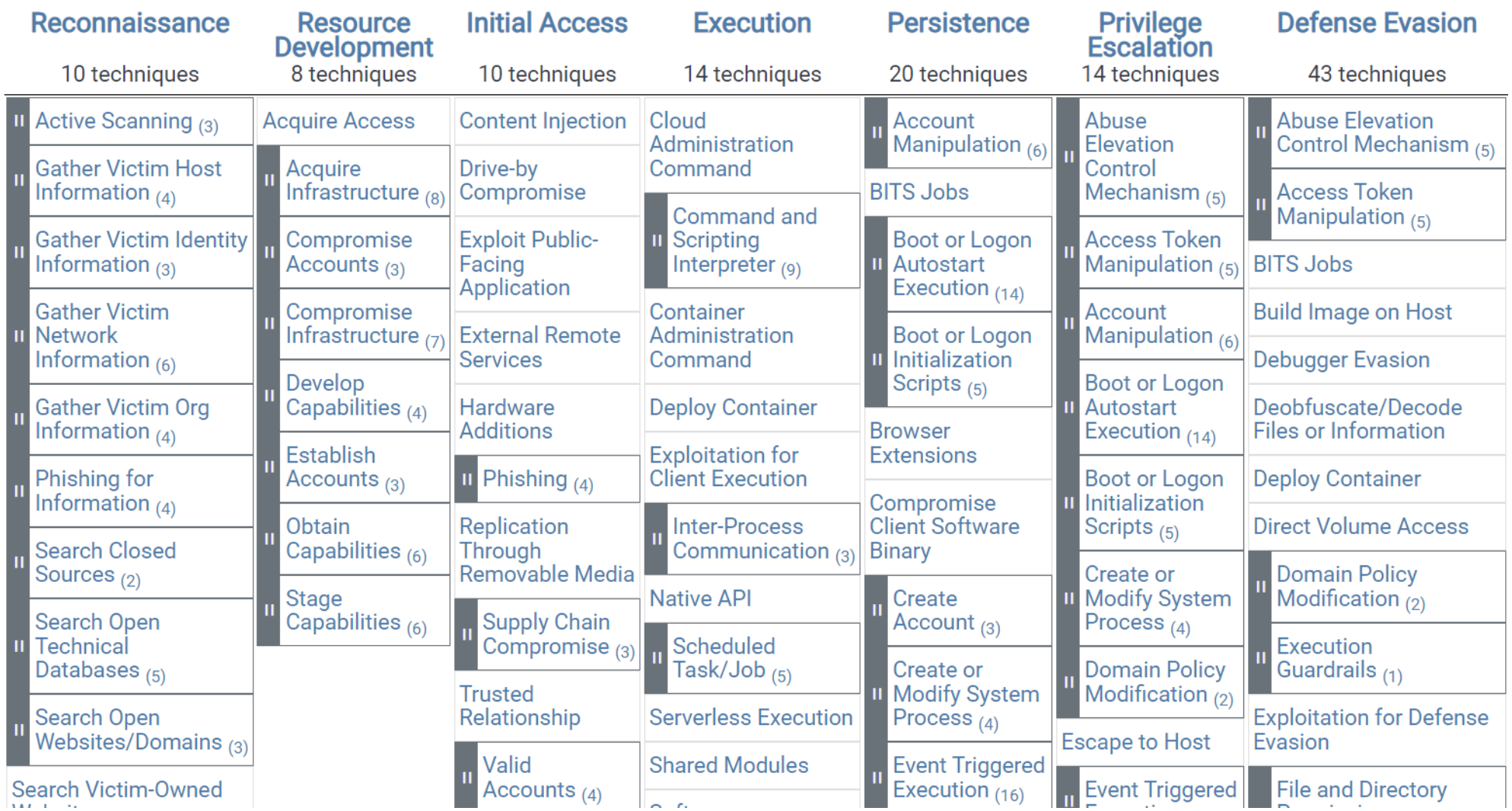
IT-Security – Und wovor schützen wir die IT?

- 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

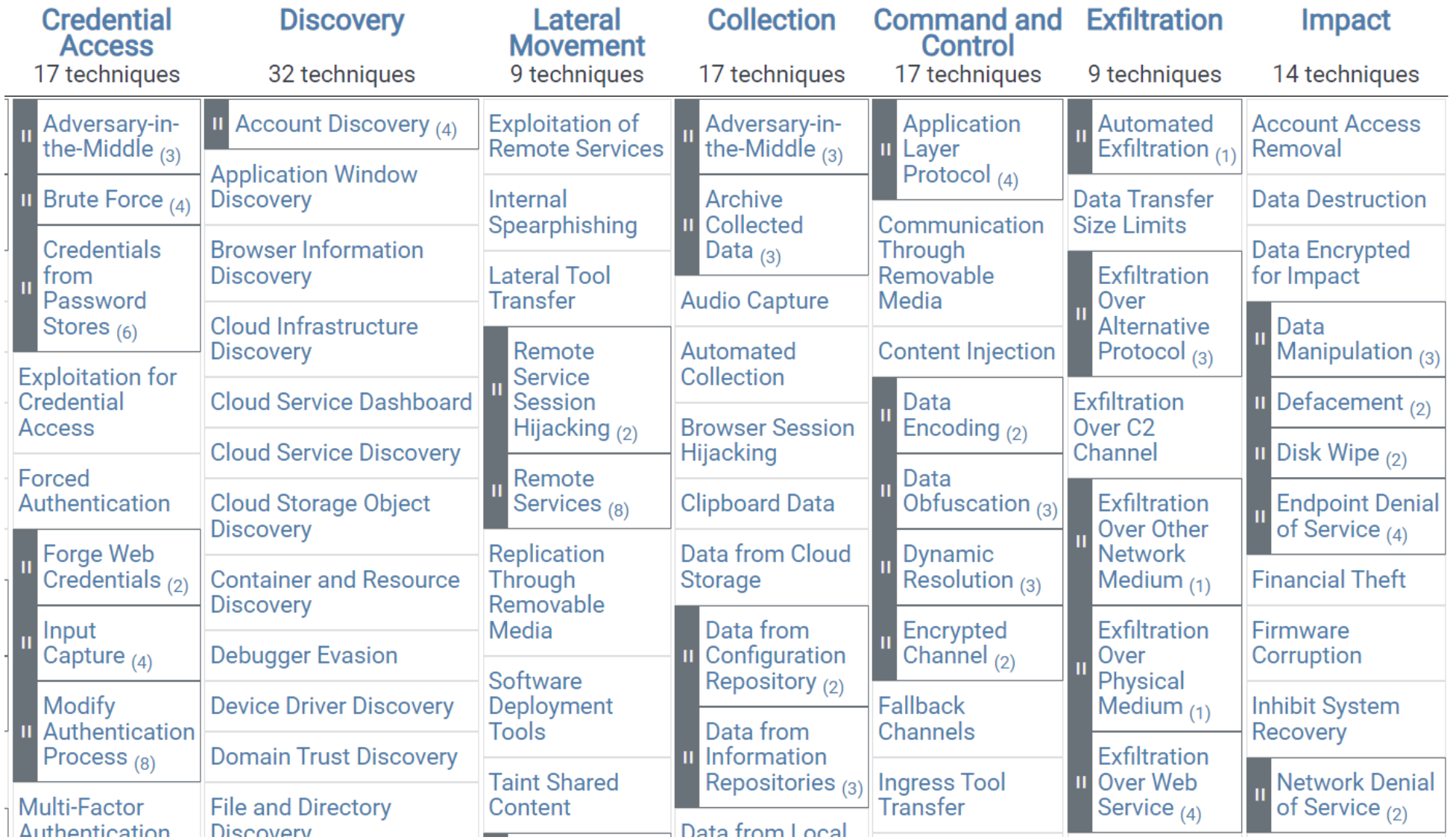
IT-Security – Was tun Angreifer denn so?

IT-Security – Was tun Angreifer denn so?



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	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)	Account Manipulation (6)	BITS Jobs
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
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Client Software Binary	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information
Search Closed Sources (2)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Create Account (3)	Domain Policy Modification (2)	Deploy Container
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (4)	Escape to Host	Direct Volume Access
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (16)	Event Triggered	Domain Policy Modification (2)
Search Victim-Owned		Valid Accounts (4)	Shared Modules			Execution Guardrails (1)
						Exploitation for Defense Evasion
						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

Stadt Wien | Wien Digital