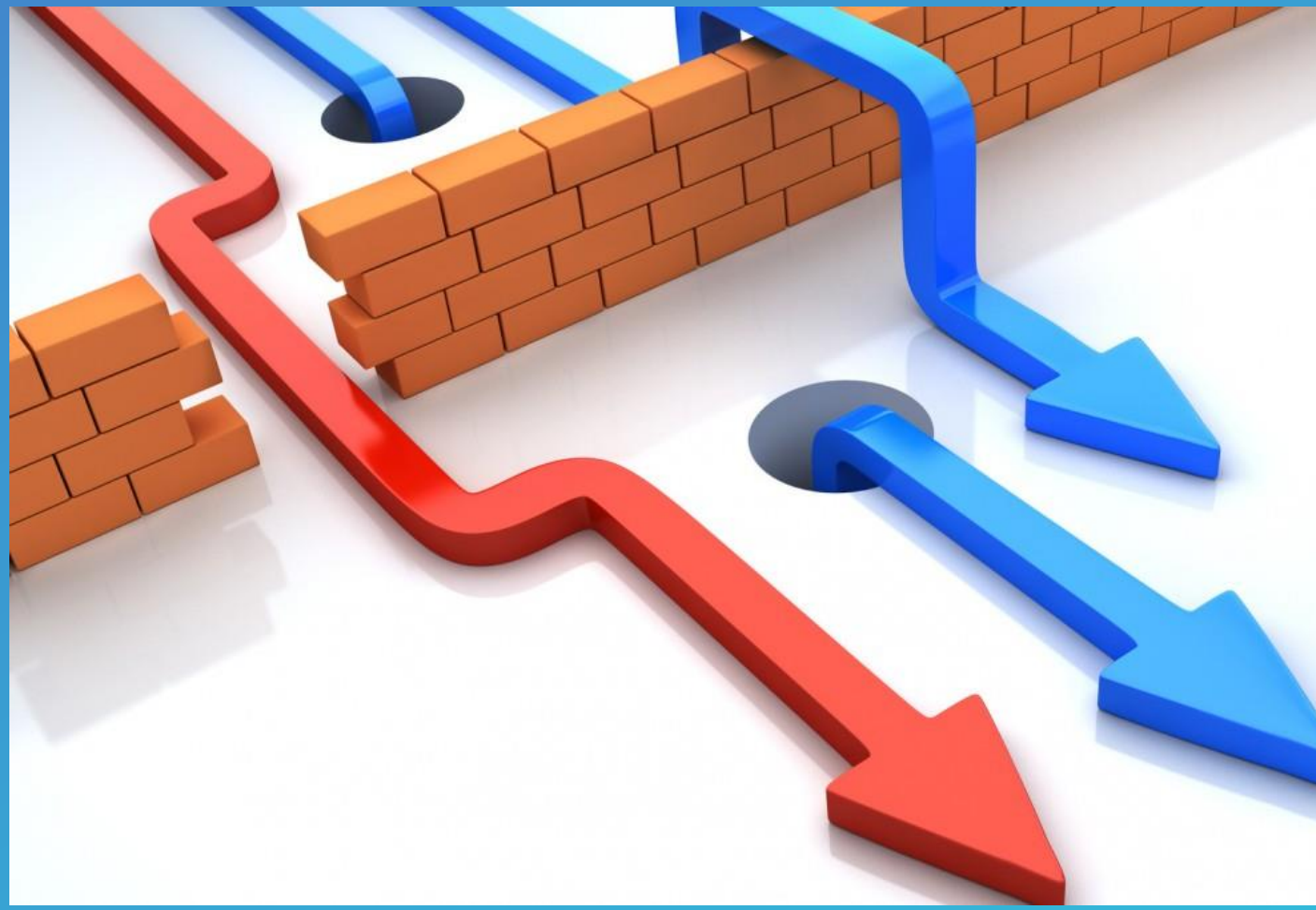
OCHRANA PRIVILEGOVANÝCH ÚČTŮ V PRAXI

sales@corpus.cz
+420 241 020 333
www.corpus.cz

Corpus Solutions a.s.
Štětkova 1638/18
140 00 Praha 4

Moderní a populární hrozby

APT (lateral movement) a vnitřní nepřítel (insider) a ...



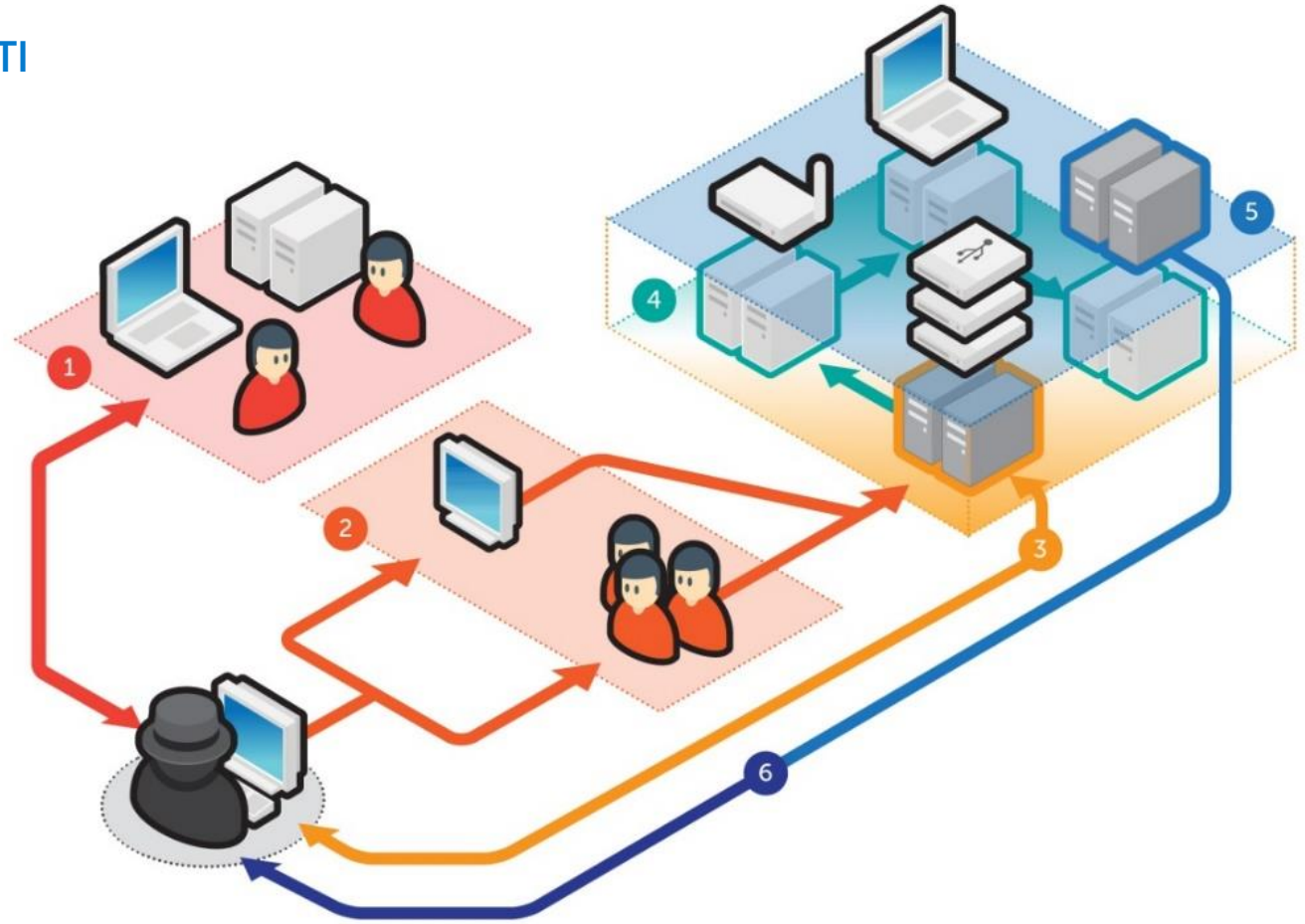
APT – Lateral Movement

O co se jedná a čím je to zvláštní?

Cílený útok a jeho šíření v prostředí oběti

Lateral Movement

- Rozšíření zájmů útočníka o další aktiva v síti oběti
- Útočník si vybírá:
  - Slabé cíle k upevnění své pozice v síti
  - Cíle, které mu zprostředkují přístup do dalších částí sítě (napříč segmentací)
  - Cíle, které umožní **získat vyšší oprávnění**
  - Hodnotné cíle k získání citlivých informací



VNITŘNÍ NEPŘÍTEL

Kdo to je a jak s ním bojovat?

ÚTOČNÍK „INSIDER“

- Oblivious
  - Viník si neuvědomil své jednání a způsobil škodu.
- Negligent
  - Nedbalostí, porušením předpisů došlo ke způsobení škody.
- **Malicious**
  - Škodlivé chování, často od zhrzeného zaměstnance. Motivací je uškodit, nebo se obohatit o informace. Často **zneužívá svá oprávnění ke klíčovým aktivům**.
- **Professional**
  - Jde si za svým cílem a pro tyto účely se nechá také zaměstnat. Zcizené informace obratem zpeněží. Často **krade privilegované účty a zneužívá přístupy**.

DODAVATEL, EXTERNÍ PRACOVNÍK, …

Někdo komu důvěřujeme

DODAVATELÉ A 3. STRANY

- Útočník často volí vektor útoku přes dodavatele. Bývají méně zabezpečeni než primární cíl
- Fluktuace pracovníků dodavatele přináší riziko úniku důležitých přístupových údajů
- Nedokumentované, nebo neschválené změny nesoucí riziko snížení dostupnosti služeb, či jejich zabezpečení
- Často chybí personifikace privilegovaných účtů = 5 pracovníků využívá stejný účet „admin“, nebo „root“

PIM / PAM

Co je to za zkratky?

PIM / PAM

Význam těchto zkratek

Privileged Identity and Access Management

- Spravuje identity pro **privilegované** účty v organizaci
- Přiděluje jednorázová hesla k jejich užívání
- Umožňuje podmínit vydání hesel potřebným workflow
- Zprostředkuje bezpečný privilegovaný přístup (jump)
- Zaznamená prováděné operace uskutečněné v přivilegovaném přístupu
- Umožní jemné nastavení oprávnění administrátorům = *každý admin nemusí mít vždy právo dělat úplně vše*

Již žádná hesla 5let stejná, na papírku, nebo v kódu aplikace!!!

PIM / PAM

Basic CIS Controls

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational CIS Controls

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational CIS Controls

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

← Technologie PIM / PAM

CIS Center for Internet Security®

Implementace PAM u zákazníka

Potřeby a motivace zákazníka

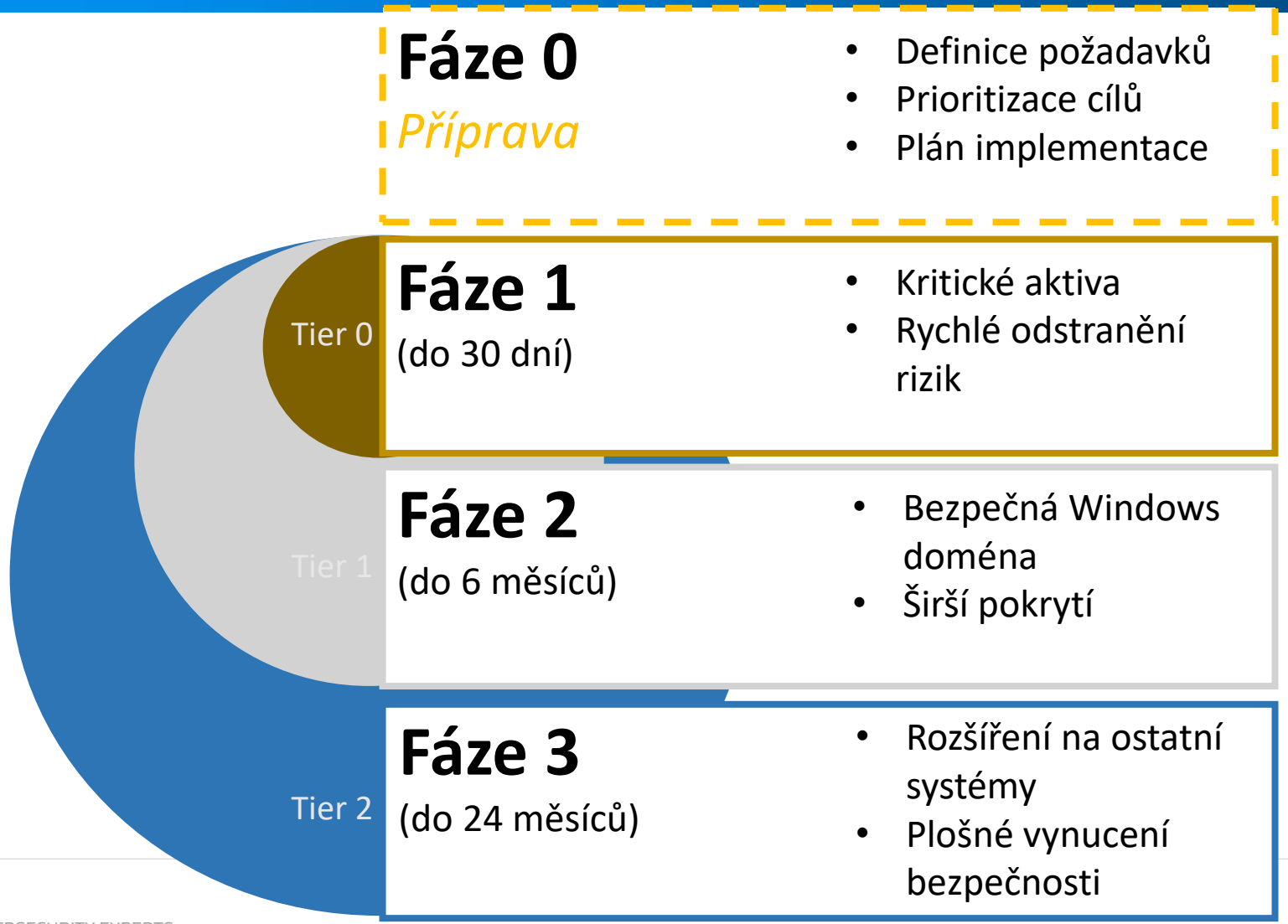
- Desítky dodavatelů s přístupem k systémům zákazníka
- Oddělení o malém počtu lidí zodpovědné za bezpečnost
- Velké množství koncových zařízení
- Složitá kontrola toho, co dodavatelé na koncových systémech dělají
- Požadavek na vysokou dostupnost připojení
- Splnění zákonných norem, nebo předpisů

Vybrané řešení – CyberArk PAS

- Centrální řízení přístupů k systémům
- Nahrávání session
- Password management (pravidelná rotace hesel)
- Bezpečné úložiště hesel, nahrávek atd.
- Silný nástroj pro kontrolu a případný zpětný audit
- Možnost napojení na systém SIEM a workflow service desku
- Zákaznické reference
- Leader na trhu
- Splnil požadavky zákazníka na jednotlivé funkcionality

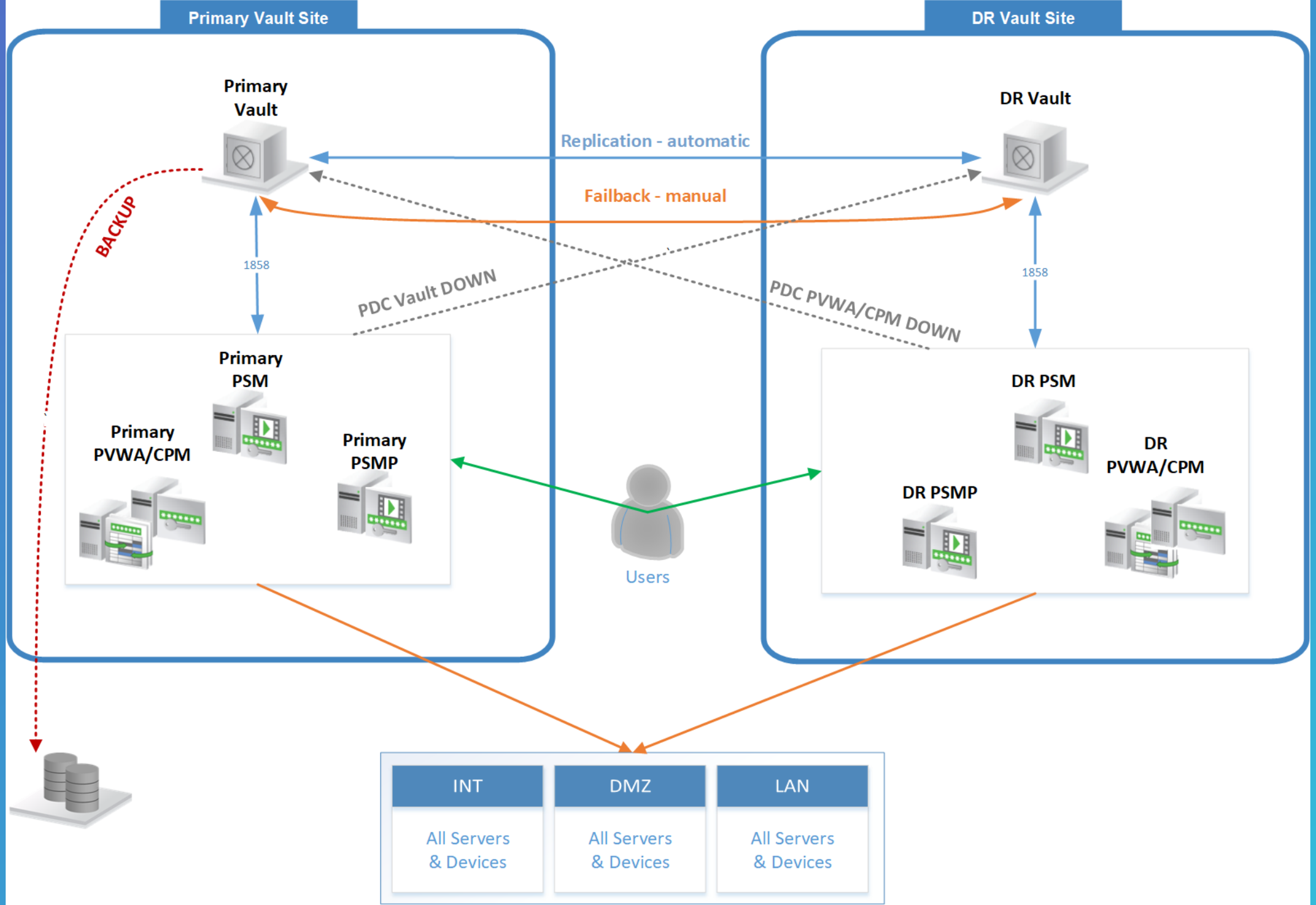
Fáze implementace zabezpečení privilegovaných účtů

PROGRAM IMPLEMENTACE



Fáze 0 – Předtím než začneme:

1. Definice požadavků
   - Eliminace kritických zranitelností – přístup k Tier0
   - Ochrana přístupu externích dodavatelů
   - Ochrana přístupů ke kritickým systémům
   - Zvýšit efektivitu správy sdílených účtů
   - Soulad s bezpečnostními normami
   - Náprava “úspěšného” kybernetického útoku
   - Identifikace rizik spojených s implementací
2. Technické požadavky
3. Identifikce a prioritizace aktiv
4. Požadavky na workflow
5. Role


Primary Vault Site
DR Vault Site
Primary Vault
DR Vault
Replication - automatic
Failback - manual
BACKUP
1858
1858
PDC Vault DOWN
PDC PVWA/CPM DOWN
Primary PSM
Primary PVWA/CPM
Primary PSMP
DR PSM
DR PVWA/CPM
DR PSMP
Users
INT
DMZ
LAN
All Servers & Devices
All Servers & Devices
All Servers & Devices

Fáze 1 – Hlavní cíle

Týden 1-2	**Příprava prostředí** **Instalace CyberArk**
Týden 3	Přístupy ke kritickým systémům a Domain Controlleru (Tier 0) • Řízení **domain admin** účtů • Monitoring aktivit, řízení přístupů a izolace relací přes PSM, vynucení 2-faktorové autentizace • Detekce podezřelých aktivit
Týden 4	Randomizace hesel pro built-in účty • ***Built - in admin účty*** – administrator, root, oracle SYS/System, enable, iLO, ..
Týden 5	Vysoce rizikové servisní účty podporované out of box • ***Vulnerability Management*** – Qualys, Rapid7, Tenable, McAfee • ***Discovery*** – Service-Now Discovery, HP Universal Discovery, ForeScout,

Fáze 1 – Příprava prostředí

	MD (Odhad)
1. Instalace CyberArk komponent	5
• Vault, Web portál - PWVA, CPM, PSM, PSMP • Hardening • Volitelné: *Load Balancing* • *Dokumentace, Testování*	
2. Integrace s infrastrukturou	2-15
• LDAP / Active Directory • Email notifikace • DR a Backupy • Volitelné: *Performance a event management, SIEM, 2-faktor autentizace, Ticketing system* • *Dokumentace, Testování*	
3. Nastavení přístupů	1-3
• Vytvoření Safes Design (např. Unix, Windows – local, Windows – Domain, ..) • Definice rolí – Vault Admin, Safe Owner, User, Auditor • Matice přístupů uživatelů do Safe	

FÁZE 1 – ŘÍZENÍ VYBRANÉ PLATFORMY

	MD (Odhad)
1. Onboarding účtů a verifikace hesel	1.5
• Nahrání účtů do CyberArk pomocí Password Upload Utility nebo Account Discovery • Verify - systém se přihlásí pomocí uloženého účtu a ověří platnost hesla (neprovádí změnu) • Získáte důvěru administrátorů – jak se pracuje s CyberArk - Seznam účtů, zobrazení a kopírování hesel, tlačítko Connect	
2. Nastavení Master politiky	1
• Frekvence výměny a komplexnost hesla • Kontrola 4 očí – zaslání požadavku na přístup k vybranému účtu • Integrace s ticketing systémem • Exkluzivní přístup • Jednorázové heslo • Email notifikace o přístupech	

FÁZE 1 – ŘÍZENÍ VYBRANÉ PLATFORMY

	MD (Odhad)
3. Password / SSH Key Management	2
• Ad-hoc změna hesel přes CPM – Tlačítko Change Now • Automatická výměna hesel na základě Master politiky • Reconciliace hesel – jak je heslo out of sync, automaticky ho změň • *Ověření pro menší skupinu účtů – následně širší nasazení*	
4. Izolace a řízení přístupů přes PSM	1-3
• Nastavení přístupů přes PSM (formou PSM, SSH Proxy, RDP Proxy, ...) • *Customizace Connection Component*	
5. *Detekce anomálií privilegovaných přístupů*	(2)
• Nastavení PTA	

Fáze 2 – Privileged Account Security Program – 1-6 měsíců

- Ochrana účtů pro kritické databáze a cloud
  - Zabezpečte databázové účty v plain textu ve WebSphere, JBOSS, Tomcat, Weblogic
  - Ochraňte důležité účty pro správu cloud prostředí

- Tiering sítě a ochrana Tier 1
  - Rozdělte aktiva do oddělených Tier prostředí (např. - Tier 0 (DC), Tier 1 (kritické servery) a Tier 2 (méně významné Servery, Desktopy))
  - Vyhrazené účty pro správu aktiv s role based access
  - Monitoring, izolace, detekce podezřelých aktivit a least privilege pre Tier 1

Fáze 3 - Privileged Account Security Program – 6-12 měsíců

- Zařazení nových účtů do CyberArk
    - Automatizace, vynucení bezpečnostných politik

- Přístupy dodavatelů přes PSM
    - Bezpečný, izolovaný a nahrávaný přístup přes PSM

Fáze 3 – Privileged Account Security Program – 12+ měsíců

- Ochrana Tier 2
  - Windows - Aplikační kontrola, Řízení oprávnění
  - Unix – Nastavení oprávnění

- Ochrana vysokorizikových servisních a aplikačních účtov
  - Popsané veškeré usages pro servisní účty
  - Definice oprávnění potřebných pro servisní účty a případné omezené (EPM)
  - Odstranění hard-coded hesel v aplikacích, skriptech

Privileged Access Management Solutions