

Organizační opatření ZKB technickým pohledem

X ALEF



§ 26	ZÁKON		ZÁKON
Nástroj pro zajišťování úrovně dostupnosti	ze dne 23. července 2014		ze dne 8. března 2017,
§ 9	o kybernetické bezpečnosti a o změně souvisejících zákonů		kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy
Bezpečnost lidských zdrojů	(zákon o kybernetické bezpečnosti)		a o změně některých dalších zákonů, ve znění pozdějších předpisů, zákon č. 181/2014 Sb.,
316			o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti),
VYHLÁŠKA			a některé další zákony
ze dne 15. prosince 2014		§ 3	§ 25
o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech,		Systém řízení bezpečnosti informací	Kryptografické prostředky
reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti		§ 30	
(vyhláška o kybernetické bezpečnosti)		Typy kybernetických bezpečnostních incidentů	
§ 10	§ 8	§ 5	§ 4
Řízení provozu a komunikací	Bezpečnostní politika		Řízení rizik
§ 32	§ 12	§ 7	
Forma a náležitosti hlášení kybernetických	Akvizice, vývoj a údržba	Stanovení bezpečnostních požadavků	
bezpečnostních incidentů		pro dodavatele	
Bezpečnost průmyslových a řídicích systémů	Řízení přístupu a bezpečné chování uživatelů	§ 28	
§ 13	§ 14	Bezpečnostní dokumentace	
Zvládání kybernetických bezpečnostních	Řízení kontinuity činností	§ 24	
událostí a incidentů	§ 16	Kontrola a audit kritické informační	Aplikační bezpečnost
§ 18	Fyzická bezpečnost	infrastrukturv a významných informačních	§ 29
Nástroj pro ověřování identity uživatelů	Kategorie kybernetických bezpečnostních	systémů	Prokázání certifikace
§ 20	§ 19	§ 17	
Nástroj pro ochranu před škodlivým kódem	Nástroj pro řízení přístupových oprávnění	Nástroj pro ochranu integrity komunikačních sítí	
§ 23	§ 22	§ 21	
Nástroj pro sběr a vyhodnocení kybernetických	Nástroj pro detekci kybernetických	Nástroj pro zaznamenávání činností kritické	
bezpečnostních událostí	bezpečnostních událostí	informační infrastruktury a významných	
		informačních systémů, jejich uživatelů	
		a administrátorů	

Typ / kategorie	Otázka
Bezpečnostní politika bezpečnost	
Politika bezpečnost	Počet datových center? Umístění: Přímá správa / outsourcována
Jsou chráněny objekty, ve kterých je umístěna DC / u umístěna DC	Obvodové oplocení, zed,...? Perimetrická ochrana? Vnější kamerové systémy?
Jsou chráněny prostory DC	Mechanické zábranné prostředky? Zařízení elektrické zabezpečovací signalizace? Prostředky omezující působení požárů? Automatické hasicí systémy? Prostředky omezující působení záplav?

Nástroje pro ochranu před škodlivým kódem	Email Antivirová ochrana pro SMTP provoz? Antispamová ochrana pro SMTP provoz? Ochrana před pokročilým malwarem? (ransomware apod.)
Přístup do internetu	Je implementována firewallová politika pro přístup do internetu? Dochází k nahrazení do SSL proxy? Má daná proxy ochranu před viry, malwarem? Dochází k filtrování URL stránek? Ochrana před pokročilým malwarem? (ransomware apod.)

Serverové operace	Nástroje pro detekci kybernetických bezpečnostních událostí Je v rámci síťového provozu implementován nástroj pro detekci kybernetických bezpečnostních událostí? - Intrusion prevention/detection system, netflow analyza apod. Jsou pravidelně kontrolovány a vyhodnocovány incidenty detekované/zablokované takovýmito nástroji?
Diskové pole (souborů)	Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí Je implementován SIEM nástroj pro sběr a vyhodnocování událostí? Jsou tyto informace pravidelně vyhodnocovány a jsou využity pro eliminaci falešné události? Existují dedikované lidské zdroje pro vyhodnocování a řešení zjištěných incidentů?
Klientské stanice	Aplikace bezpečnost (tyká se aplikací dostupných z vnější sítě) Jsou prováděny aplikační testy zranitelnosti před implementací nových aplikací? - OWASP, Rapid7, Nessus Jsou prováděny aplikační testy zranitelnosti po jejich změně/aktualizaci? Je nasazená trvalá kontrola aplikací a informací dostupných z vnější sítě před neoprávněnou činností? - v případě webových aplikací např. web application firewall

Kryptografické prostředky	Směrnice Jsou vytvořeny vnitřní směrnice pro řízení kryptografických prostředků? Jsou vnitřně specifikovány povolené šifry a jejich minimální síla z hlediska délky klíče a jejich typu?
---------------------------	--

Nástroje pro integritu komunikačních sítí	Perimetrový FW Ano/ne? Oddělení aplikací/služeb do separátních DMZ? Jsou firewally v clusteru?
Datacentrový FW	Ano/ne? Jsou firewally v clusteru? Oddělení vnitřních DC sítí? Oddělení uživatelských sítí?
Síťová architektura	Rozdělení aplikací a logických celků do separátních VLAN? (aplikační, databázová, prezentační)
VPN	Jsou využity VPN brány? Jaká technologie? (IPsec, SSL, ...) Typy šifrovacích a hashovacích algoritmů? Řízení přístupu? Řízení oprávnění do sítě?

Nástroje pro zaznamenávání činnosti infrastruktury	Síťová infrastruktura Jsou logovány události na síťových prvích? Je logován typ události, datum, čas, typ činnosti, ID původce a místa, úspěšnost/neúspěšnost? Jsou tyto informace zasílány do centrálního nástroje? Centrální sběr logů Jsou tyto informace chráněny před neoprávněnou změnou nebo čtením? Je logováno přihlášení a odhlášení správců/uživatelů? Je logována činnost administrátorů? Jsou logovány změny přístupových práv? Logování neprovedení činnosti v důsledku nedostatku práv? Logování zahájení a ukončení činnosti (start a ukončení služby)? Logování automatická varovná nebo chybová hlášení? Logování přístupy k logům, manipulace s nimi, změny nastavení logování? Logování změny hesel? Jsou logy uchovávány déle než 3 měsíce? Je synchronizován systémový čas nejméně 1x za 24 hodin? Např.: NTP
Serverová infrastruktura	Jsou logovány události na serverech? Je logován typ události, datum, čas, typ činnosti, ID původce a místa, úspěšnost/neúspěšnost? Jsou tyto informace zasílány do centrálního nástroje? Centrální sběr logů Jsou tyto informace chráněny před neoprávněnou změnou nebo čtením? Je logováno přihlášení a odhlášení správců/uživatelů? Je logována činnost administrátorů? Jsou logovány změny přístupových práv? Logování neprovedení činnosti v důsledku nedostatku práv? Logování zahájení a ukončení činnosti (start a ukončení služby)? Logování automatická varovná nebo chybová hlášení? Logování přístupy k logům, manipulace s nimi, změny nastavení logování? Logování změny hesel?

Autentizace na síťové prvky	Centrální Protokoly? Autentizační databáze? Minimální délka hesla? Vynucení složitosti? (3 ze 4 - velké, malé písmeno, číslice, speciální znak) Expirace hesla? Je možné měnit heslo častěji než 1x za 24 hodin? Uzamčení relace při nečinnosti? Jiné zabezpečení - 2FA - Smart Cards?
Lokální	Sdílené účty? Minimální délka hesla? Vynucení složitosti? (3 ze 4 - velké, malé písmeno, číslice, speciální znak) Expirace hesla? Je možné měnit heslo častěji než 1x za 24 hodin? Uzamčení relace při nečinnosti? Jiné zabezpečení - 2FA - Smart Cards?

Nástroje pro ověřování identity uživatelů	Autentizace na síťové prvky Centrální Protokoly? Autentizační databáze? Minimální délka hesla? Vynucení složitosti? (3 ze 4 - velké, malé písmeno, číslice, speciální znak) Expirace hesla? Je možné měnit heslo častěji než 1x za 24 hodin? Uzamčení relace při nečinnosti? Jiné zabezpečení - 2FA - Smart Cards?
Lokální	Sdílené účty? Minimální délka hesla? Vynucení složitosti? (3 ze 4 - velké, malé písmeno, číslice, speciální znak) Expirace hesla? Je možné měnit heslo častěji než 1x za 24 hodin? Uzamčení relace při nečinnosti? Jiné zabezpečení - 2FA - Smart Cards?

Nástroje pro ověřování identity uživatelů	Autentizace na síťové prvky Centrální Protokoly? Autentizační databáze? Minimální délka hesla? Vynucení složitosti? (3 ze 4 - velké, malé písmeno, číslice, speciální znak) Expirace hesla? Je možné měnit heslo častěji než 1x za 24 hodin? Uzamčení relace při nečinnosti? Jiné zabezpečení - 2FA - Smart Cards?
Lokální	Sdílené účty? Minimální délka hesla? Vynucení složitosti? (3 ze 4 - velké, malé písmeno, číslice, speciální znak) Expirace hesla? Je možné měnit heslo častěji než 1x za 24 hodin? Uzamčení relace při nečinnosti? Jiné zabezpečení - 2FA - Smart Cards?

Nástroje pro ověřování identity uživatelů	Autentizace na síťové prvky Centrální Protokoly? Autentizační databáze? Minimální délka hesla? Vynucení složitosti? (3 ze 4 - velké, malé písmeno, číslice, speciální znak) Expirace hesla? Je možné měnit heslo častěji než 1x za 24 hodin? Uzamčení relace při nečinnosti? Jiné zabezpečení - 2FA - Smart Cards?
Lokální	Sdílené účty? Minimální délka hesla? Vynucení složitosti? (3 ze 4 - velké, malé písmeno, číslice, speciální znak) Expirace hesla? Je možné měnit heslo častěji než 1x za 24 hodin? Uzamčení relace při nečinnosti? Jiné zabezpečení - 2FA - Smart Cards?

303 otázek

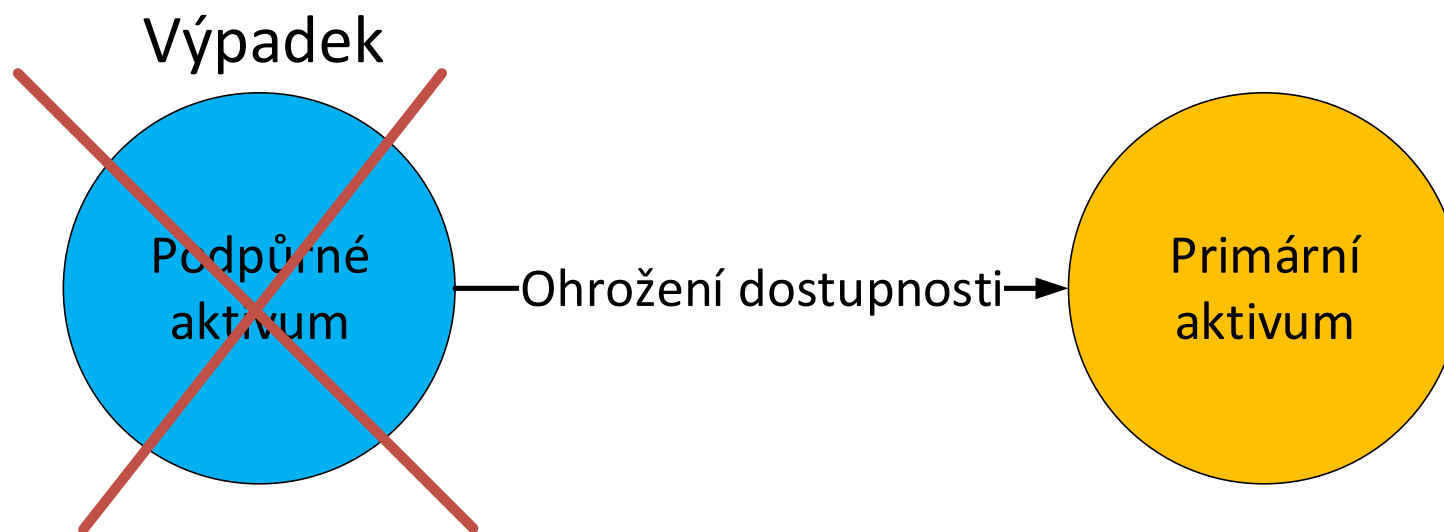
- Jak zhodnotit současný stav?
- Kde aplikovat technická opatření?

- Významný informační systém
- Kritická informační infrastruktura
- ISZS – Informační systém základních služeb
- Informační systém
- Komunikační systém
- Primární aktiva
- Podpůrná aktiva

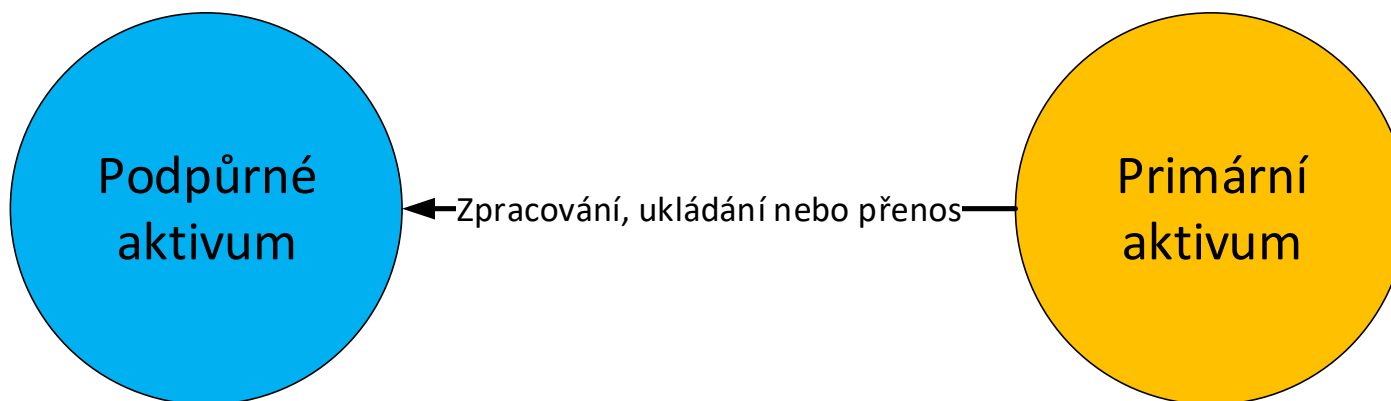
Co je podpůrné aktivum?

- podpůrná aktiva jsou technická aktiva, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního systému
- technickým aktivem je technické vybavení, komunikační prostředky a programové vybavení informačního systému

Jak poznat podpůrné aktivum

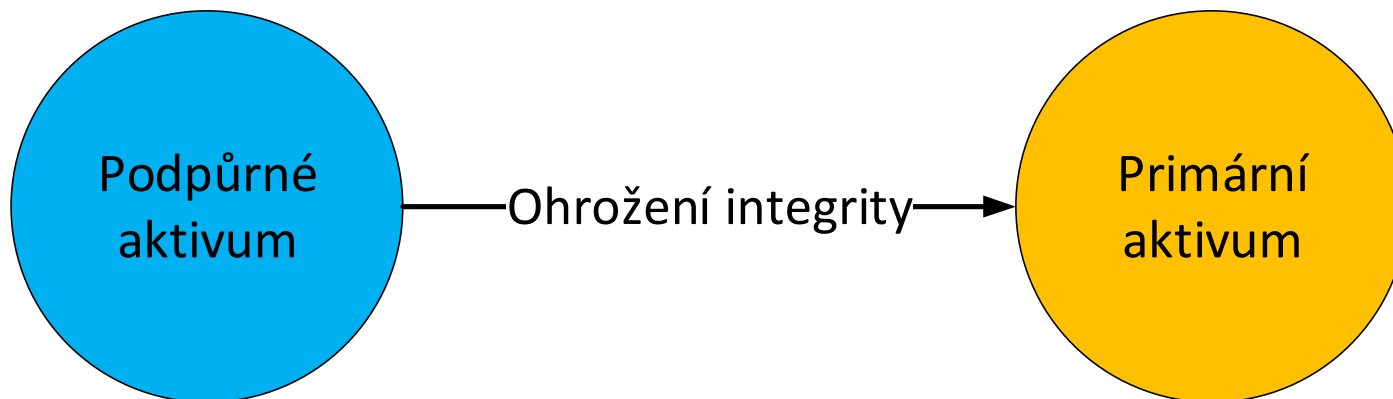


Jak poznat podpůrné aktivum

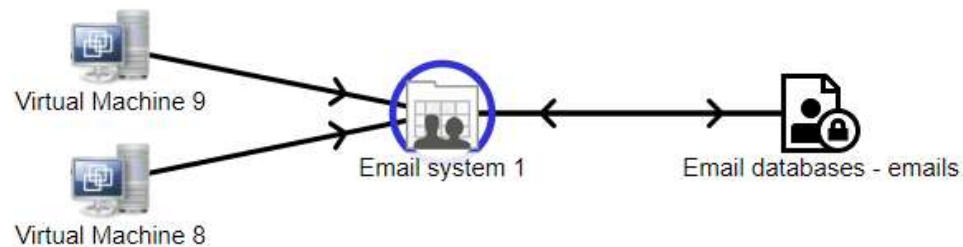


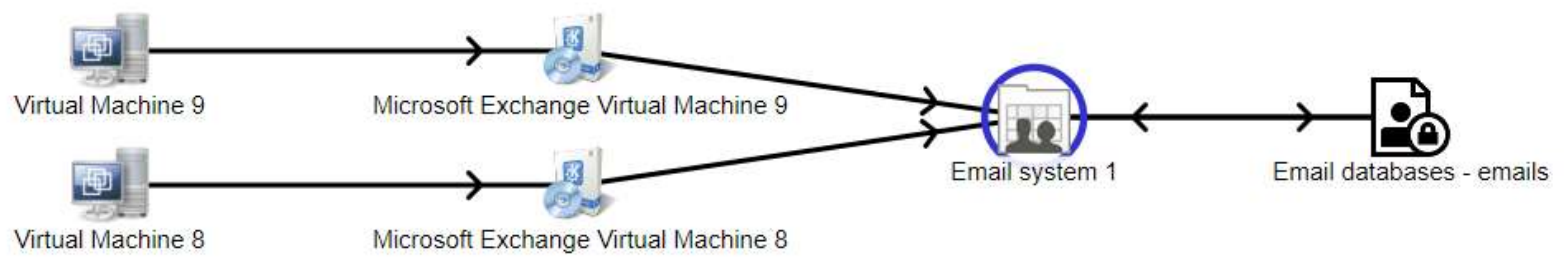
Jak poznat podpůrné aktivum

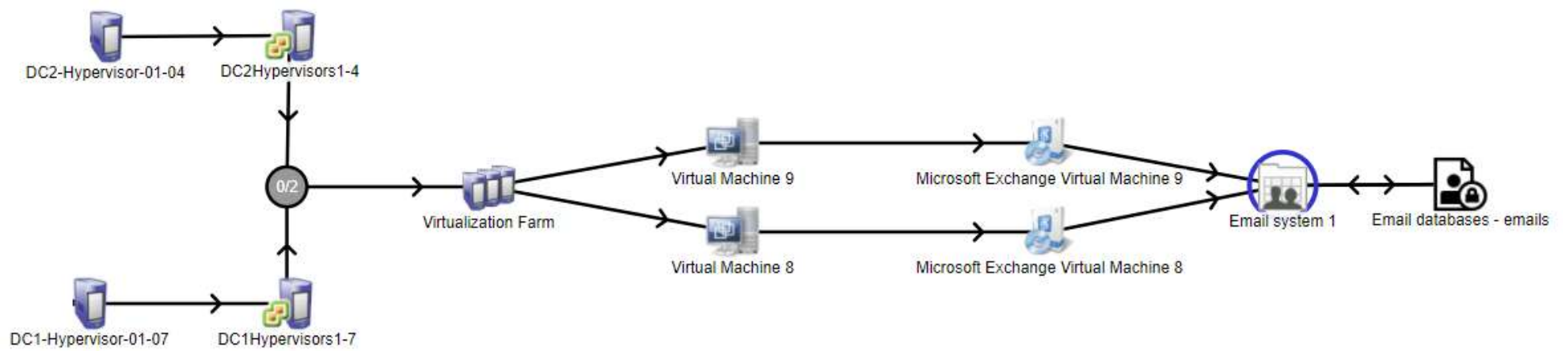
Kompromitace

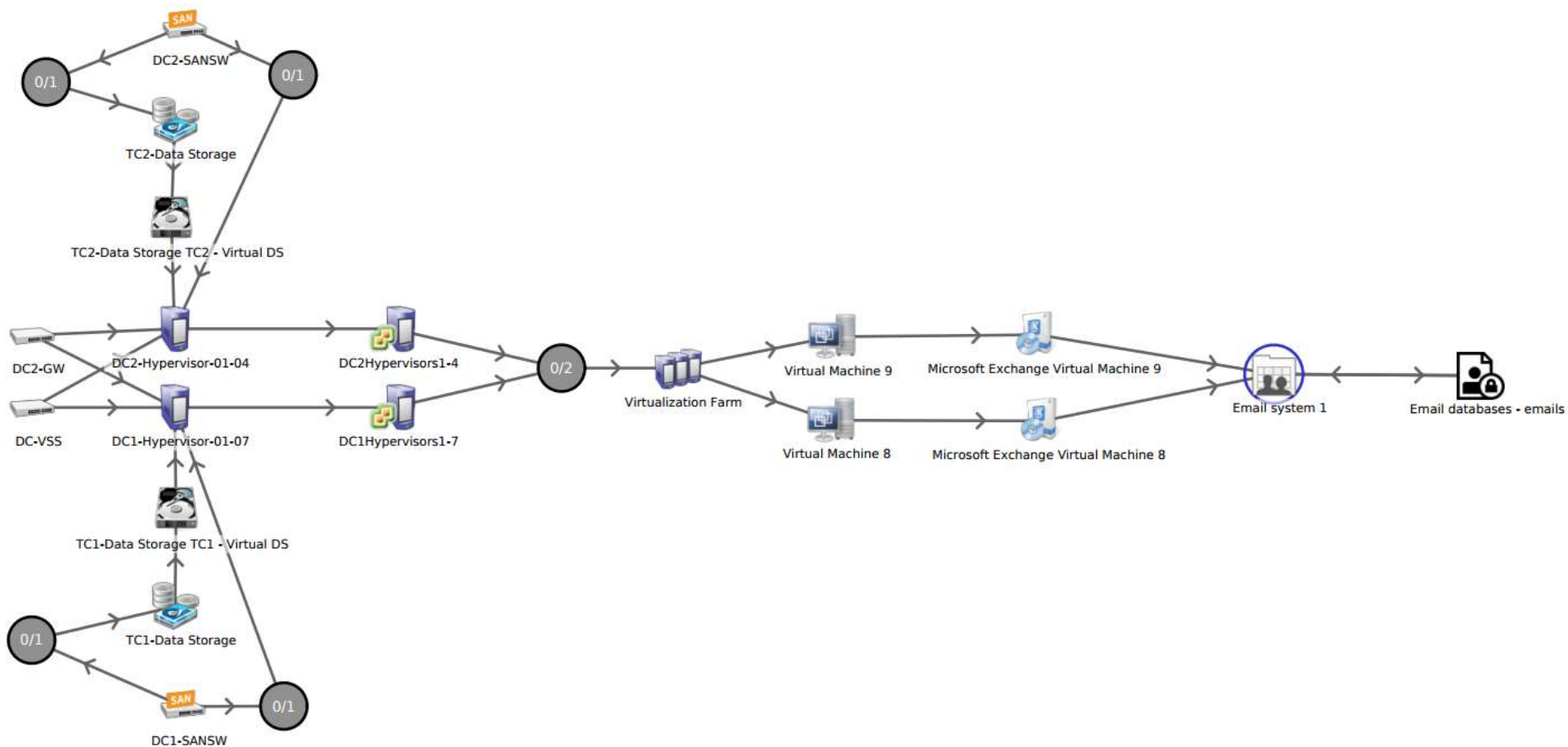


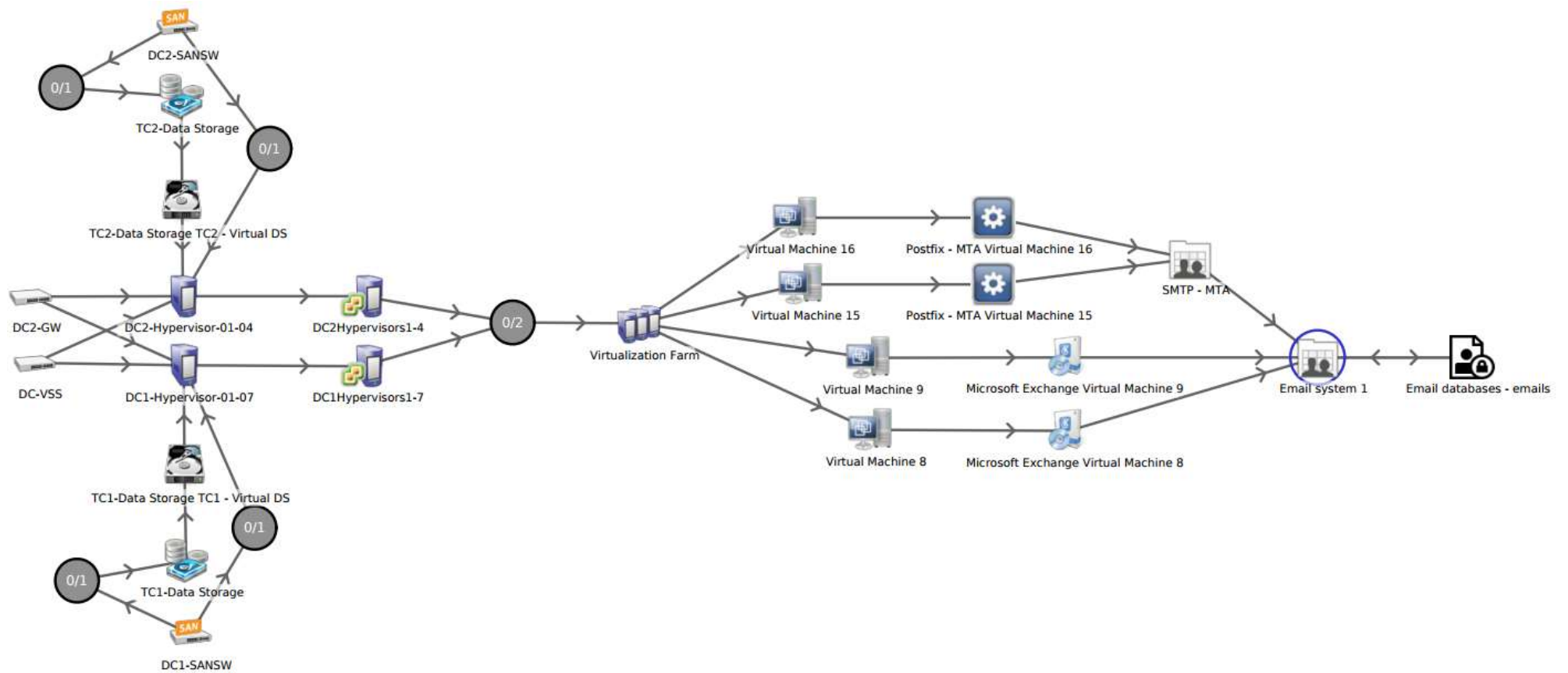
Analýza podpůrných aktiv

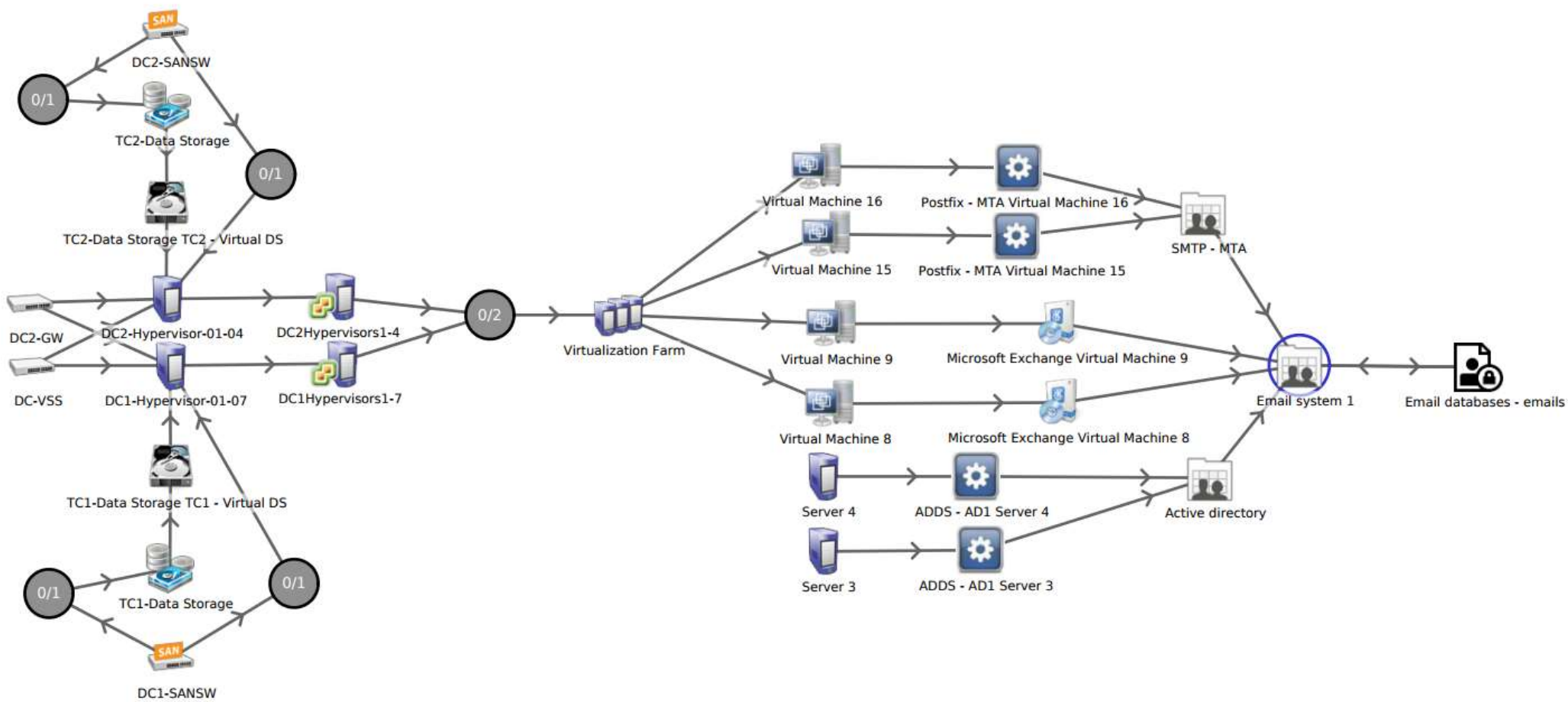


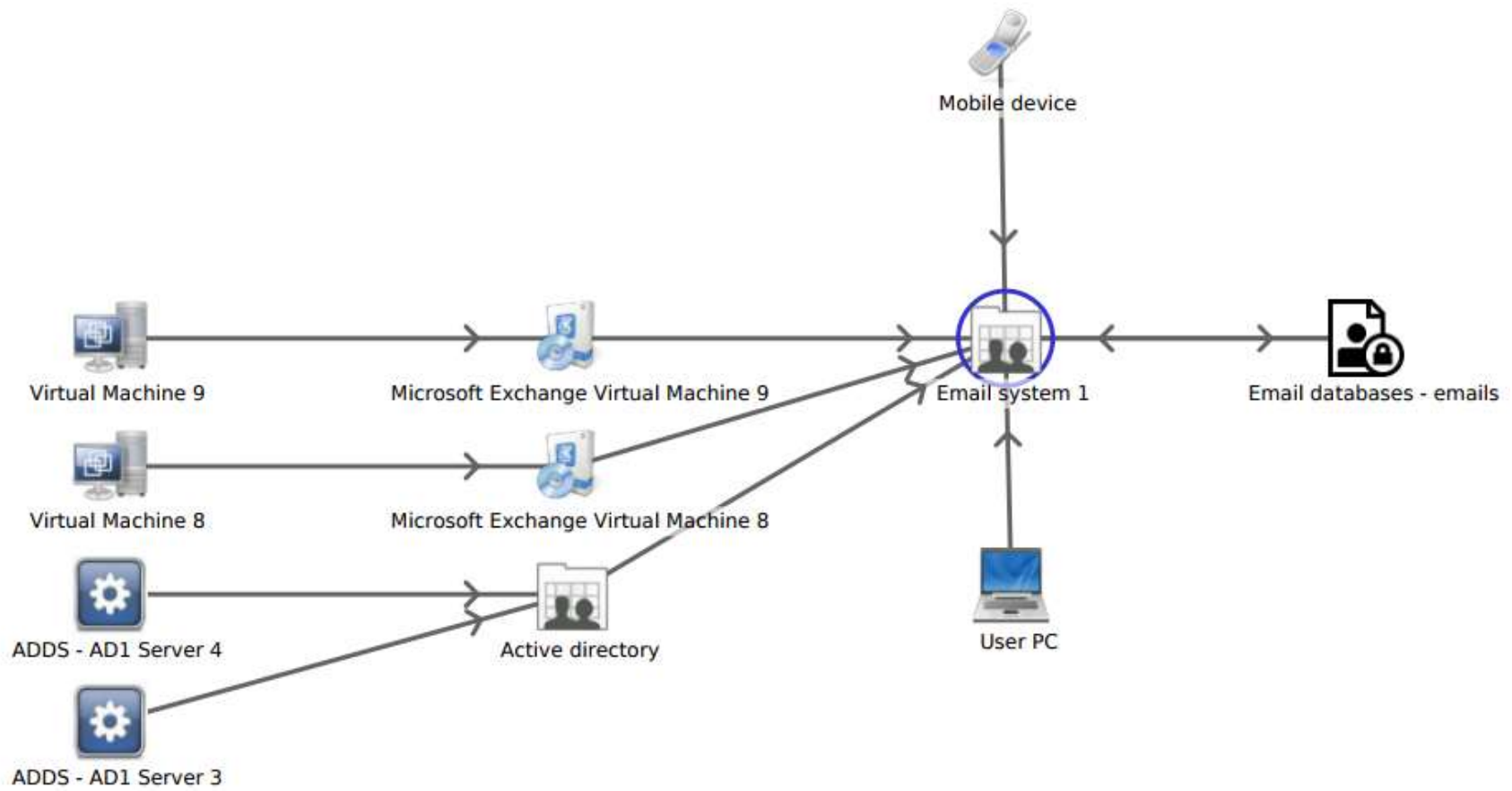


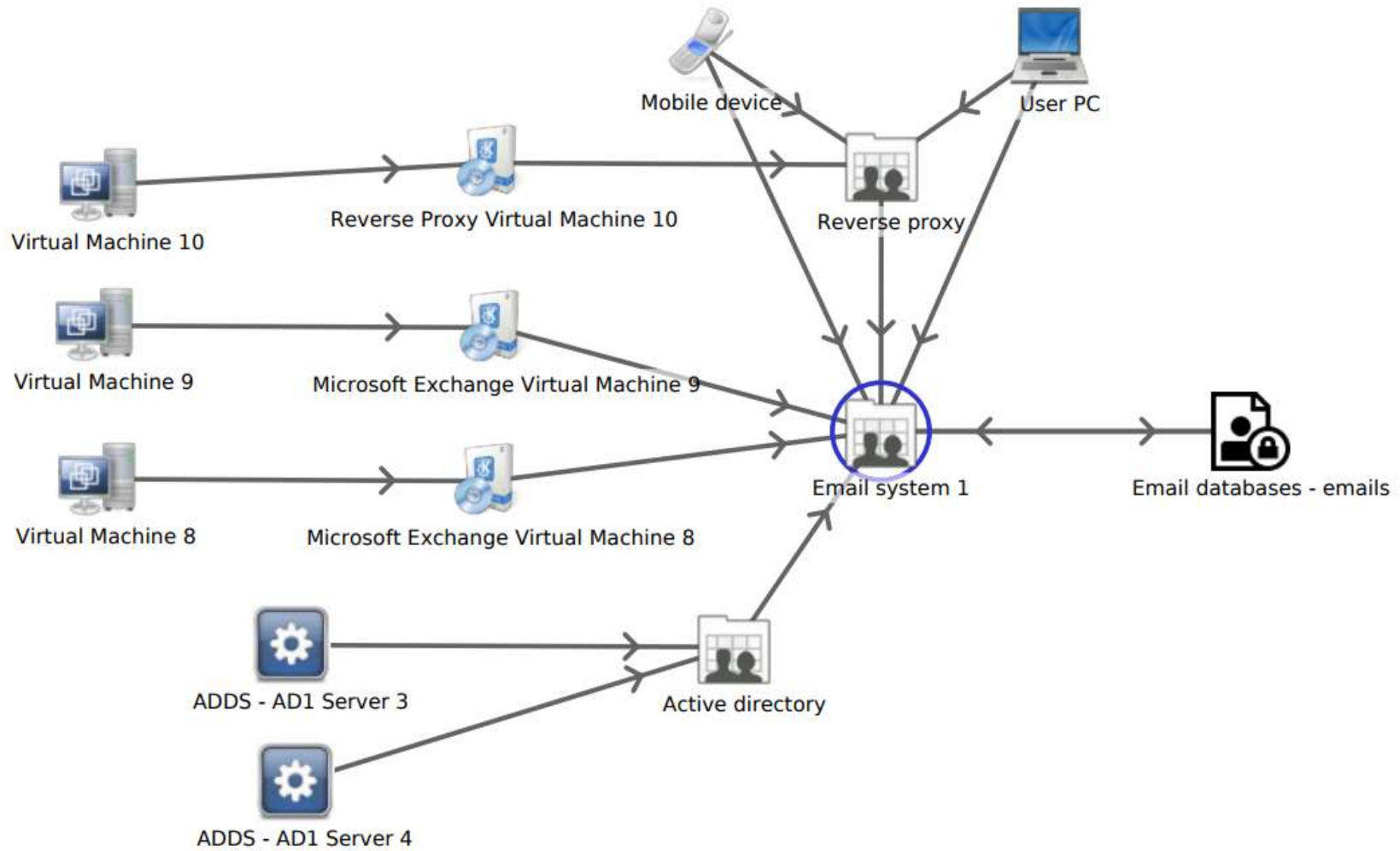


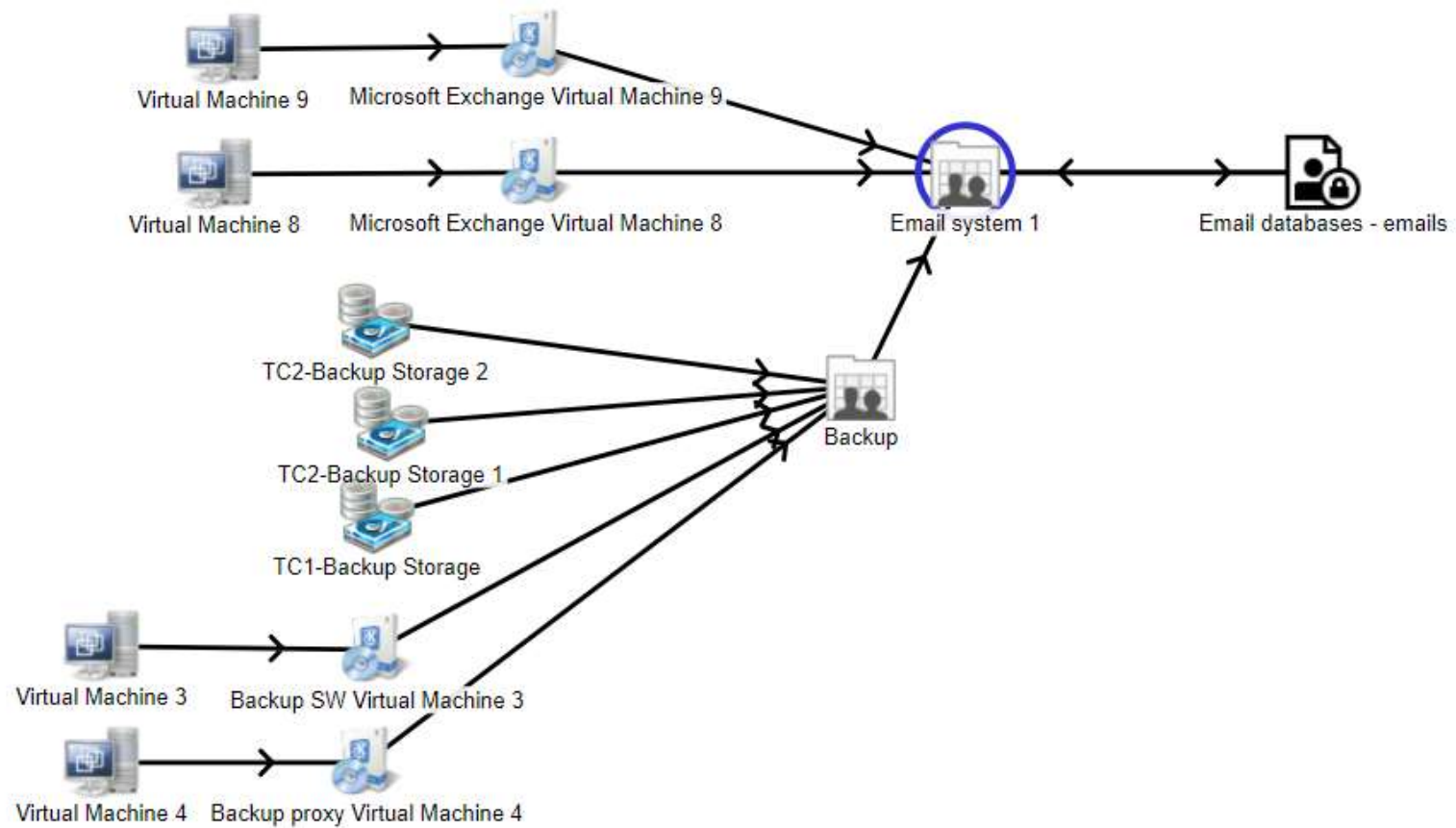


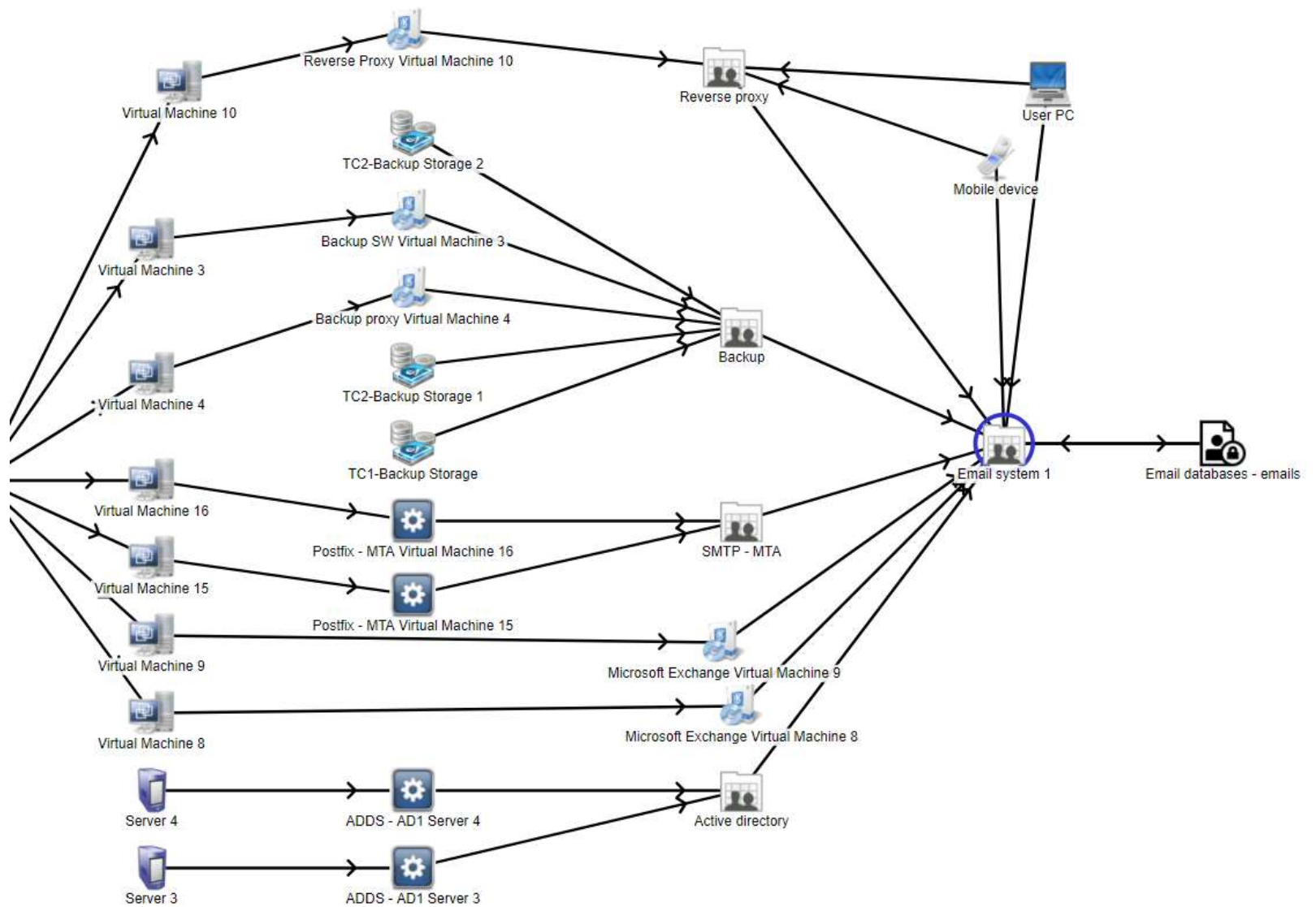


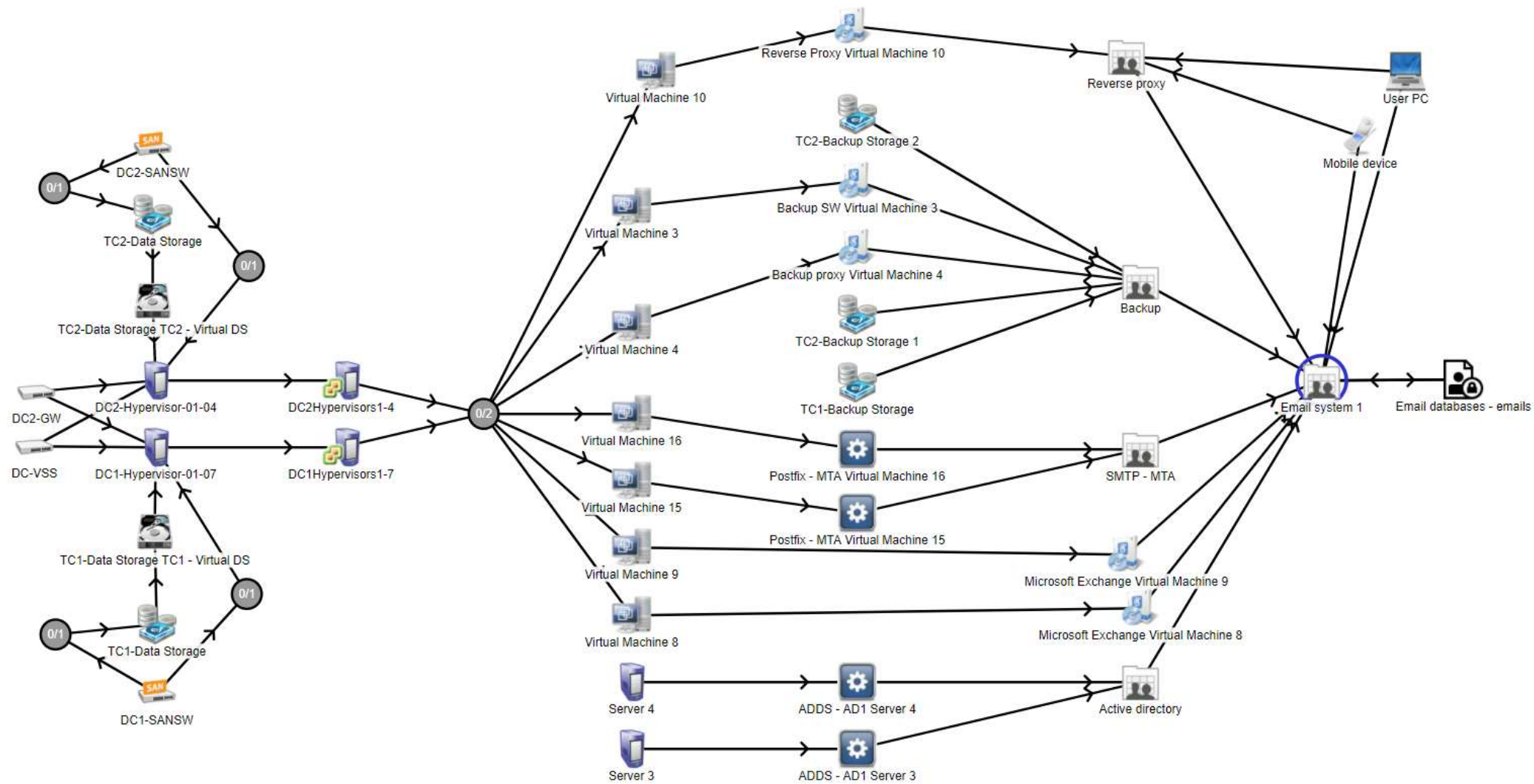




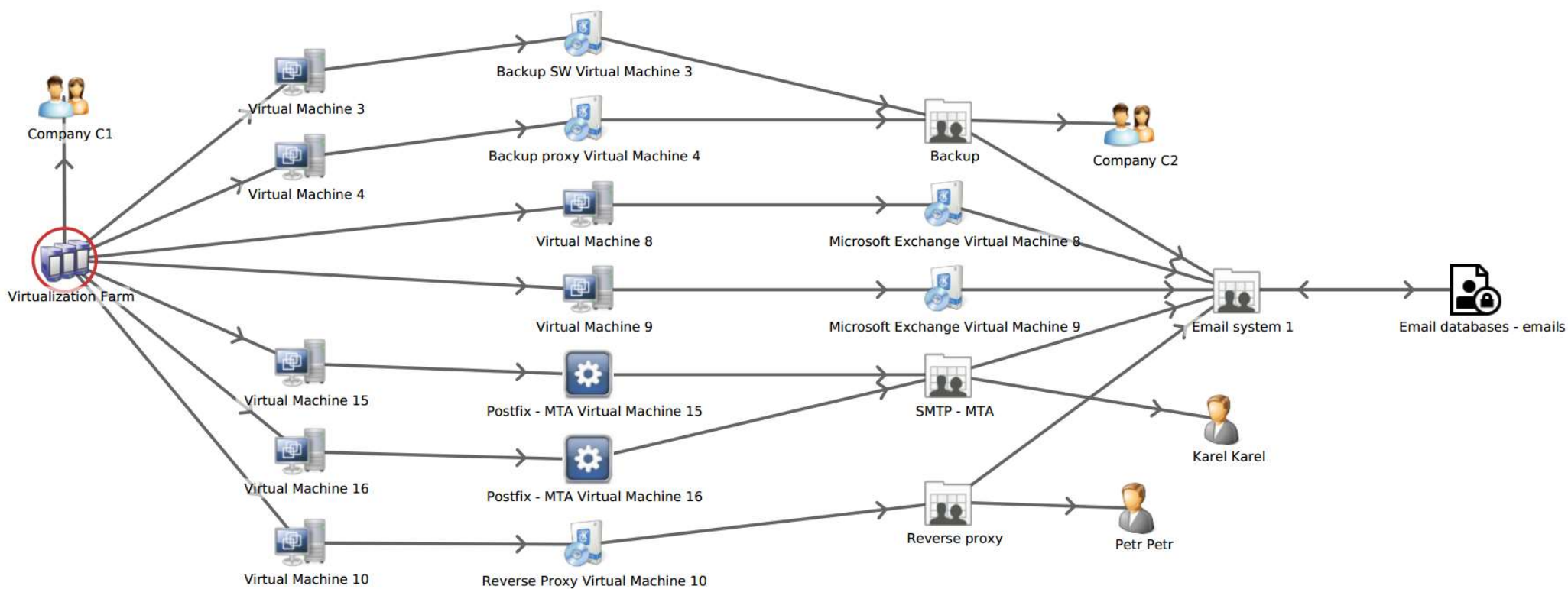


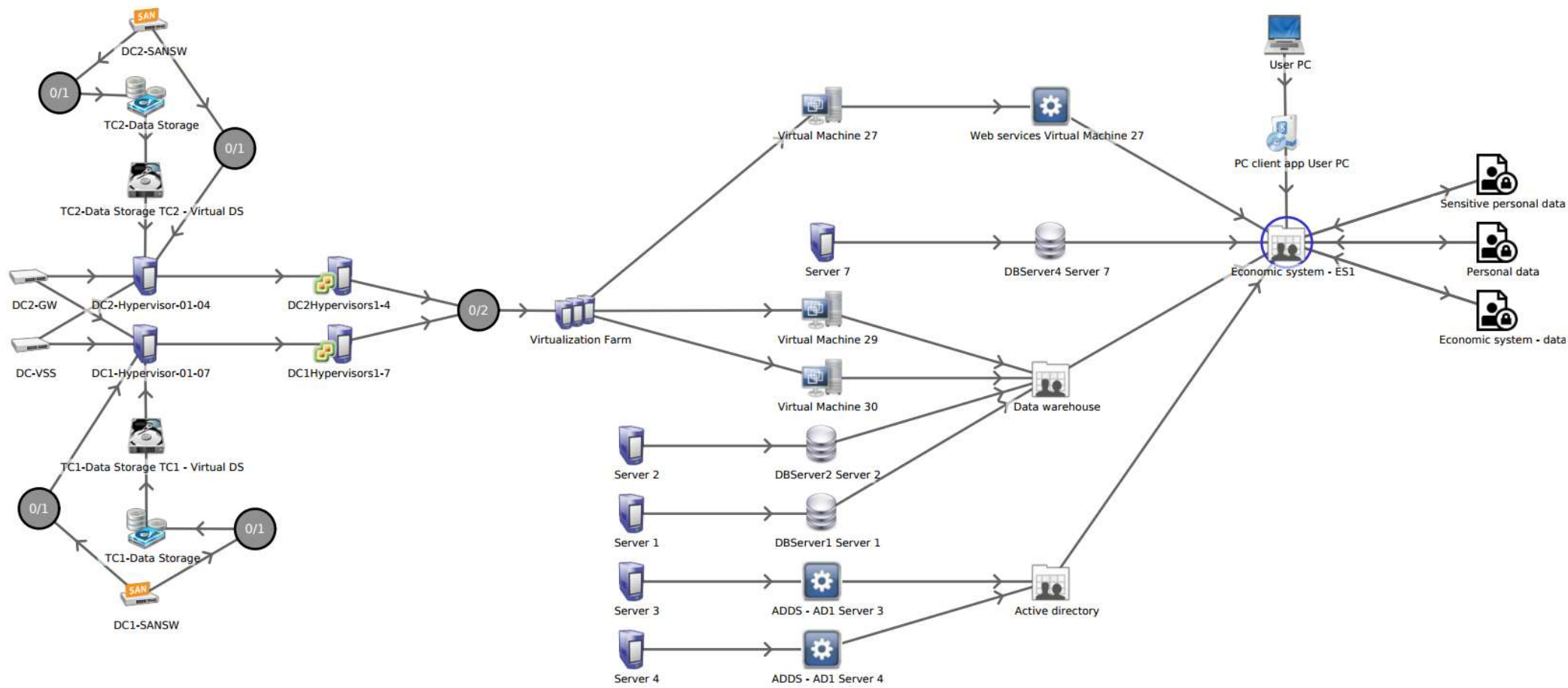


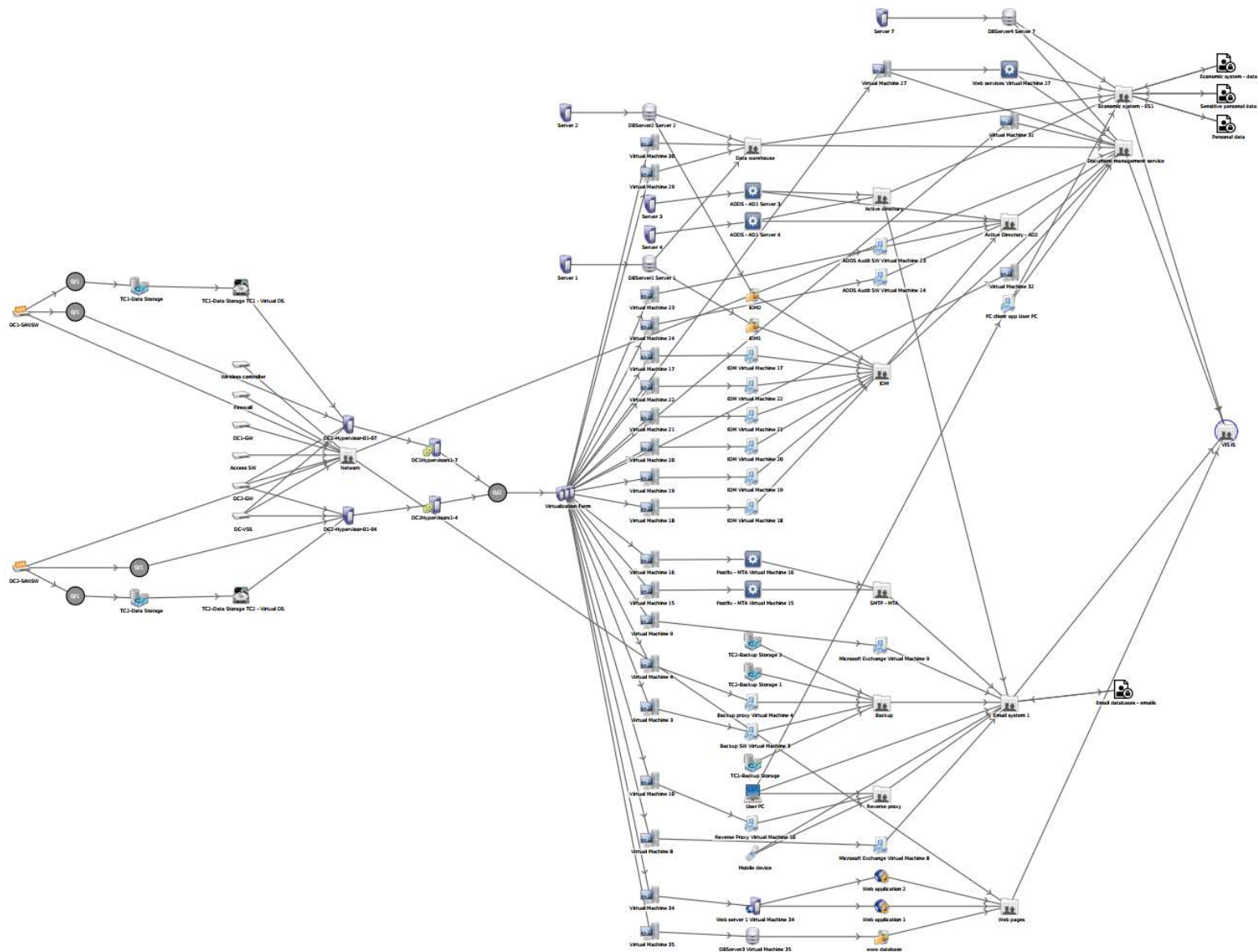




Další příklady







- Pro implementaci vhodných organizačních a technických opatření je nutné znát skutečný rozsah a vazby odvozených podpůrných aktiv v ISMS, tak aby opatření byla efektivní

Využití

Modely jsou vhodné pro:

- Návrh ISMS
- Implementace ISMS
- Provoz ISMS
- Audit ISMS

Kontakt



Martin Hubínek
Systems Engineer, Security

martin.hubinek@alef.com
www.alef.com

ALEF NULA, a.s.
U Plynárny 1002/97
101 00 Praha 10
Czech Republic





Děkuji za pozornost