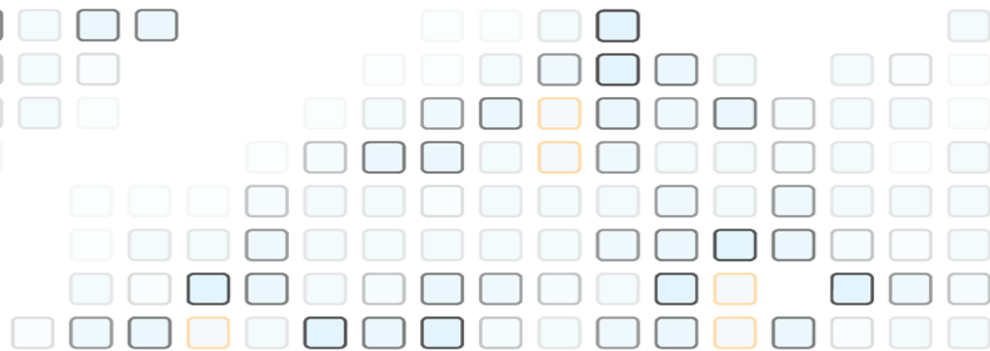


IS/STAG
is-stag.zcu.cz



Bezpečný vývoj, bezpečný provoz, bezpečná správa? Bezpečný audit!

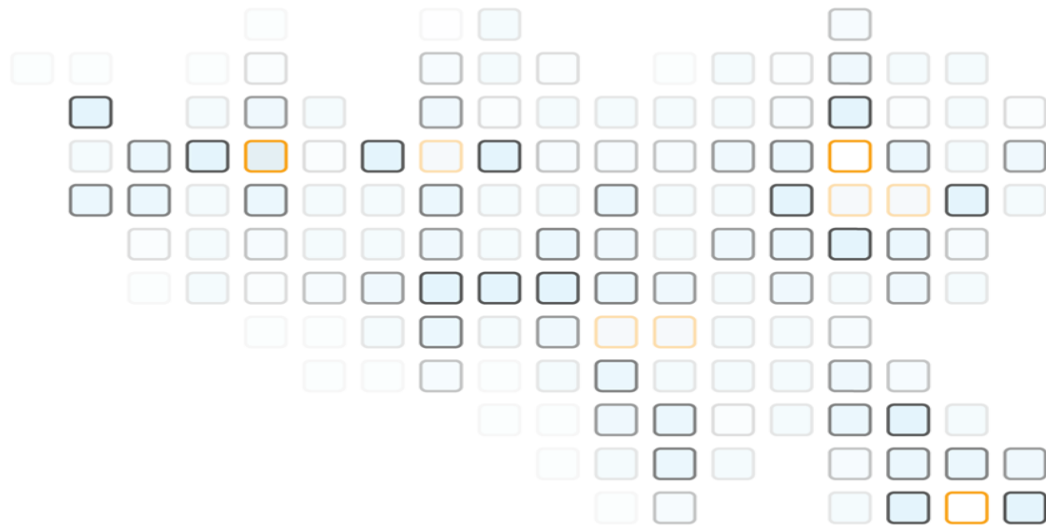
Jan Krňoul, carney@civ.zcu.cz
vedoucí týmu webových vývojářů

Poděkování sponzorům

Národní plán obnovy pro oblast vysokých škol pro roky 2022 - 2024

Agenda

- Na podzim 2025 jsme na ZČU absolvovali audit KB (CESNET z.s.p.o.)
- Podklady pro váš audit KB
 - Naše prezentace pro auditory
- Zkušenosti z našeho auditu (MKB zprostředkovaně)
- Přílepek: zabezpečené přístupy



Audit kybernetické bezpečnosti

Jan Krňoul, carney@civ.zcu.cz
vedoucí týmu webových vývojářů

Program

- **Úvod, co je IS/STAG**
 - Technologický stack - DB, servery, klienti, personální zabezpečení
 - Provoz - on premise / outsourcing
- **Vývoj - řízení změn**
 - Cyklus vývoje - nové fce / opravy chyb
 - Automatizace, testování, distribuce
 - SLA a požadované reakční doby (smlouva)
- **Vývoj - základy bezpečného vývoje**
 - best practices, metodiky, vliv prostředí
 - předávání zkušeností
 - pentesty
 - komponenty a knihovny třetích stran a jejich pravidelné vyhodnocování
- **Provozní bezpečnost**
 - Aktualizace jednotlivých SW komponent (DB, OS, web server, knihovny)
 - Produkce / vývoj / demo
 - Osobní údaje na vývoj / demu
 - Správa hesel / credentials na serverech
- **Vlastnictví a správa dat**
 - Administrátoři
 - Audit v rukách administrátorů, logy a jejich uchovávání
 - "Datová" bezpečnost, vnitřní kontroly
- **Zákazníci a komunikace**
 - směrem k nám (požadavky na nové fce a rozvoj, hlášení chyb)
 - směrem od nás (nové fce, opravy chyb), newsletter
 - pravidelná školení a semináře

Úvod, co je IS/STAG

- Informační systém pro administraci studijní agendy vysoké školy a univerzity
 - Studijní programy a plány, předměty, studenti a studia, zkouškové termíny, rozvrhy, přijímací řízení, absolventi, platby - závazky a pohledávky
- Široká paleta modulů
- Napojení na infrastrukturu univerzity a systémy třetích stran
 - IdM, SSO, spisové služby, SIMS, e-learning, anti-plagiátorské systémy, knihovny, ISZR
- Vývoj ZČU, nasazení a provoz aktuálně na 15 školách ČR
- Pro veškeré úpravy i nové funkce preference stability a udržitelnosti před novinkami

Úvod, používané technologie

- Databázový systém Oracle, má výlučné postavení
 - Integrita dat, řízení přístupů (student, vyučující, vyšší role - SR, fakulty)
 - Omezení tam definovaná nelze obejít z klientských aplikací (viz dále)
- Windows klient (UIS) pro klíčové uživatele (referentky, tajemníci, ...)
 - "Tlustý klient", Oracle technologie (DB + backend)
- Web pro širokou masu uživatelů (studenti, vyučující, vedení školy)
 - Portál IS/STAG, Java stack, interní vývoj
 - OS (Debian), běhové prostředí Java (OpenJDK 21), Web server Tomcat
 - Spring framework
- Webové služby pro napojování a integraci dalších IS
 - Interní vývoj, sdílení komponent s Portálem
- Dvě jednoúčelové Java aplikace (Editor rozvrhů a Editor plánů)
- Mobilní aplikace různých dodavatelů, prostřednictvím WS
- Provoz - DB, Web, WS
 - Na lokální infrastruktuře školy ("on premise") - větší školy
 - "Outsourcing", na infrastruktuře ZČU - menší školy (cca 1500 studentů)
- Na ZČU produkční, vývojové, testovací prostředí
 - Dále "demo" - veřejné, na pokusy, veškeré os. údaje anonymizované
 - Obvykle mají školy vlastní produkci + test / demo, podle potřeb

Řízení změn a vývojový cyklus

- Databáze: vlastní distribuční mechanismus, zabezpečený kanál, přístup výhradně z IP segmentu vývojářů
- Windows klient a "Editor": Vlastní distribuční mechanismus, automatické aktualizace při spuštění
- Web a WS: Testování sestavených verzí (automat, podle existujících scénářů)
- Web a WS: Vlastní distribuční mechanismus, nasazení podle potřeb škol (v nočních hodinách, některé školy nasazují opožděně a testují samy), *bezvýpadkové*
- Každých 14 dní vydání "release" (1. a 15.) - nové funkce, opravy chyb
 - Před vydáním několik dní testovací provoz na produkčním prostředí ZČU
 - Během dalšího období oprava jen konkrétní chyby, *žádné nové funkce*
 - "Opakovatelné" buildy (stejná závislosti, stejný kód)
- Smluvní SLA - reakční doby pro výpadky, odstraňování vážných / lehkých závad (hodiny / dny)

Vlastní vývoj

- Version control (Git + GitLab na infrastruktuře ZČU), build (Gradle) a deployment management (vlastní nástroj)
 - Řízení přístupu vývojářů ke kódu - několik repozitářů (DB, Web, TeX)
- Statická analýza kódu - součást IDE IntelliJ Idea
- Interní framework pro formulářové aplikace (cca 10 let+, validace a kontroly)
- Omezení SQLInjection útoků (prepared statements, *je pracnější vytvořit zranitelný kód než bezpečný*)
- Ochrana proti CSRF a CORS útokům na úrovni portálu
- Možnost XSS také omezena prostředky portálu
- Pravidelné penetrační testování (2016, 2020, 2025)
 - Nálezy mají sestupnou tendenci (poprvé velmi závažné nálezy [RCE a kompromitace prostředí], naposledy jeden nález [neautorizovaný přístup k datům uchazeče])
 - White box testing (zdrojové kódy, přístup k infrastruktuře)
 - Navíc i přes zákazníky v rámci testování jejich infrastruktury
- Zabezpečení vývojářských stanic - i ty jsou cílem pentesů
 - Přístupy přes VPN
- Potenciální riziko - SW třetích stran - knihovny a frameworky
 - Vývojáři sledují security bulletiny / zranitelnosti
 - Konzervativní strategie zavádění nových verzí
- Stabilní a zkušený tým, fungující předávání know-how a zaučování nových sil

Provozní bezpečnost

- Jednotná "platforma"
 - DB: stejná verze, odpovědnost správců
 - ZCU: čtvrtletní Oracle security patche, vážné zranitelnosti ihned, správce aktivně sleduje
 - Windows klient: Weblogic, podobný režim jako DB
 - Pro web: OS (Debian 12) + Java + web server (Apache Tomcat)
 - Rozdělení kompetencí a jasné hranice
 - OS: automatické bezpečnostní aktualizace, správce systému sleduje
 - Java a Tomcat: starší prověřené verze, pravidelné revize zranitelností, vývojáři aktivně sledují
 - Vždy řízený upgrade (testování, domluva se zákazníky)
 - Stabilní a udržitelné prostředí přednost před novými funkcemi (HTTP/2).
- Oddělené prostředí - provoz, vývoj, test, samostatné řízení přístupů
 - vývoj a test db a portál nejsou přístupné mimo IP segment CIV / Admin VPN
 - Pravidelná rotace hesel
 - Demo prostředí veřejné, pro uživatele ZČU, další zákazníky i zájemce o IS/STAG, veškeré osobní údaje anonymizované (zachovány vazby)
 - Web: Omezený přístup k credentials na serverech, (hesla, klíče a tokeny)
- Uživatel ⇔ Webové rozhraní vždy šifrovaný kanál (https)
- Přístupy do produkčního prostředí - administrátoři IS/STAG (viz dále)
- Uživatelské role (cca 45) + příslušnost k pracovišti
 - Role určuje dostupné funkce
 - Pracoviště určuje dostupná data

Vlastnictví a správa dat

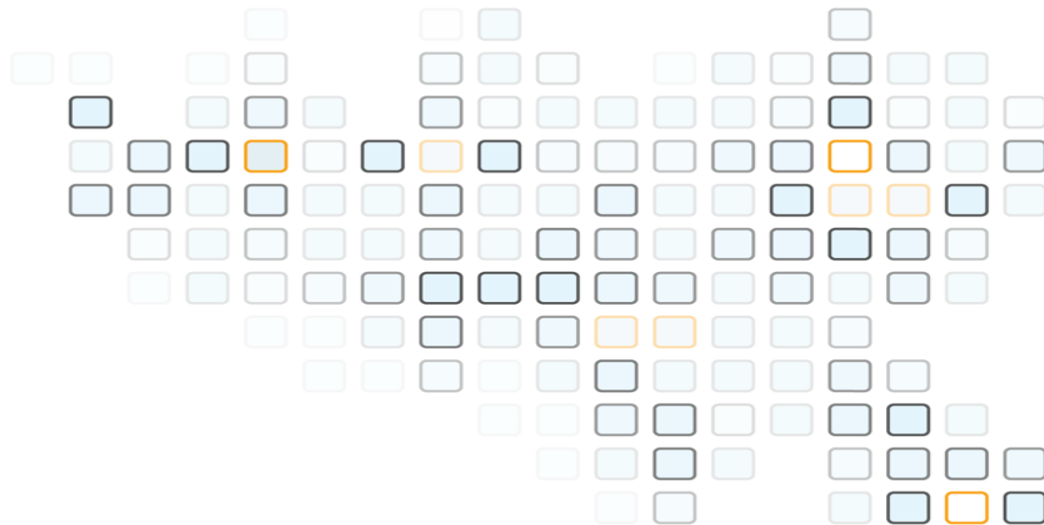
- IS/STAG (data) je ve správě školy, vždy existuje administrátor / oddělení odpovědné za IS/STAG
- Administrátor řídí přístupy do produkce (konta), pro web vazba na SSO, vyšší role přímo DB konta
- K dispozici aplikační "Audit"
 - Zaznamenávání veškerých změn dat na DB úrovni (kdo, kde, kdy, jak)
 - Velká režie (objem dat), proto musí administrátoři explicitně zapnout a udržovat
 - Uchovávání věcí školy / správců (např. pravidelné kopie do jiných tabulek)
- Administrátorsky dostupné logy a protokoly (DB)
 - Pro kritické operace, integrace a napojování
 - GUI nástroj, filtry - oblast, čas, ...
 - Velká režie (objem dat), proto musí administrátoři explicitně zapnout a udržovat
 - Uchovávání 6 měsíců, pro vybrané oblasti (EWP) déle
- Aplikačně závislé logy (soubory na FS)
 - Více věc vývojářů (logování aplikací)
 - Uchovávání v rámci "platformy" 24 měsíců
- Existuje sada pravidelně spouštěných "kontrol", zaměřeno primárně na přehledy, statistiky, chyby a konzistenci dat
 - Ale i duplicitní identity, chyby ve výkazech, neplatné parametry...

Zákazníci a komunikace

- Smluvně určené kontakty pro obě strany
 - Dotazy / požadavky a náměty / hlášení chyb
 - RT fronty (Request Tracker), administrátor školy
- Vždy vyžadován ticket v RT - záznam řešeného problému
 - Administrátoři mohou sledovat stav všech svých ticketů
 - A do jisté míry i cizích (informovanost)
 - Reporting a hlídání nedořešených věcí, specifikace priorit a řízení správcí
 - Priority, historie zpráv, časové odhady, náročnosti, vlastně projektové řízení
 - Uživatelé ale mají možnost jednoduchého hlášení chyb
- Pravidelný "Seminář IS/STAG" na jaře
 - Malá konference (cca 80 účastníků, 2,5 dne), zveme zástupce škol - administrátory a vedení škol, často vedoucí studijních referátů
 - Prezentování malých i velkých novinek
 - Plány a vize do budoucna
 - Velký prostor pro dotazy, diskuse a osobní jednání
- Letní konzultační dny v Plzni (cca 2 dny), prezentace zásadních novinek a osobní konzultace
- Setkání studijních prorektorů škol s IS/STAG
- "Komunita" - správci / školy spolupracují a komunikují mezi sebou
- Pravidelné návštěvy na školách - on-site školení (cca den na školu a rok)
- S každou verzí zasílaný Newsletter IS/STAG
 - Novinky ve verzi, opravy chyb, "marketing"
- Produktový web, administrátorská a uživatelská dokumentace, systémová příručka, veřejná a neveřejná část

Doplnění z minulého týdne

- ZoKB v prováděcí vyhlášce nařizuje sledování zranitelností
- Děláme to, vizte předchozí slidy, vizte výsledky pentestů, komunikaci / RT
 - Ale živelně, nejspíše bude potřeba zpracovat politiky, metodiky a dokumentaci, ...



Audit prakticky

Zvládli jsme to my, zvládnete to taky

Zkušenosti z průběhu

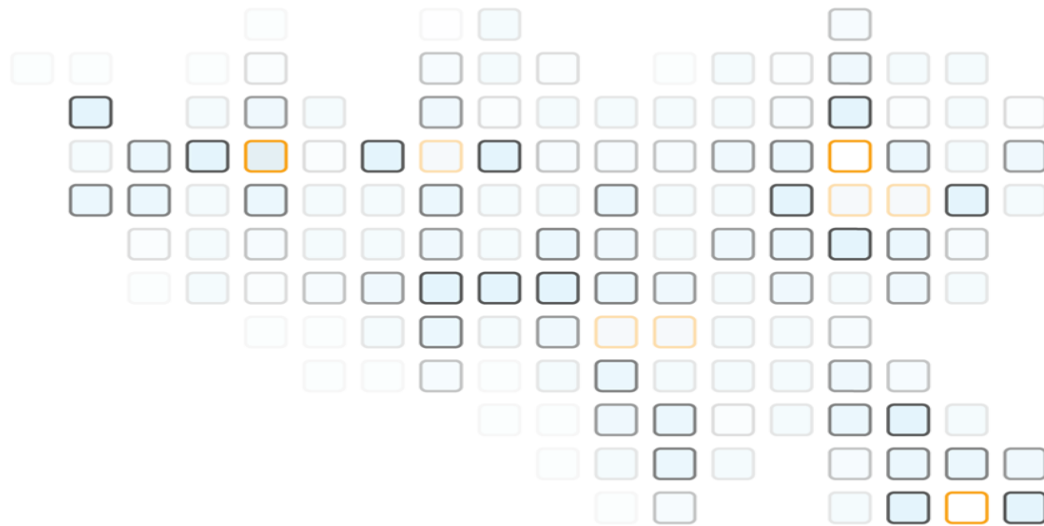
- Průběh auditu - CESNET
 - Jeden den, 4 "auditoři"
 - Audit celého IT / CIV, ne jen STAG
 - Po celý den prezentace + diskuse s garanty oblastí / systémů
 - cca 30 minut okno => byl jsem jeden z mnoha
- Návaznost na vnitřní audit univerzity
 - ostatní složky univerzity
 - manažer bezpečnosti (ne jen kyber-)
 - vazby na vedení

Závěry a výsledky

- (zprostředkovaně, od našeho MKB)
- Výchozí teze
 - Za běžných okolností se vás auditor nesnaží nachytat
 - (Naopak, je rád, když je všechno v pořádku)
- Dobrá nevyžádaná rada
 - Projevte iniciativu - připravte program sami, nečekejte na otázky, snažte se tomu jít naproti
 - Příprava, iniciativa (security officer)
- My sami jsme do toho šli s tím, že technicky máme vše OK, ale máme mizernou dokumentaci
- Dopadlo to dobře (= žádné překvapení)

Citáty na závěr

- Auditor je taky člověk, nechce se dívat na chudáka, co se tam potí a neví
 - Trochu jako revizor v MHD, taky se s vámi nechce prát
- Je třeba ukázat že i když nemáš papíry, tak v praxi to funguje dobře
- Přejde další audit (prostor pro zlepšení)



BKI (aneb síťáři milují zkratky)

Bezpečná komunikační infrastruktura IS/STAG

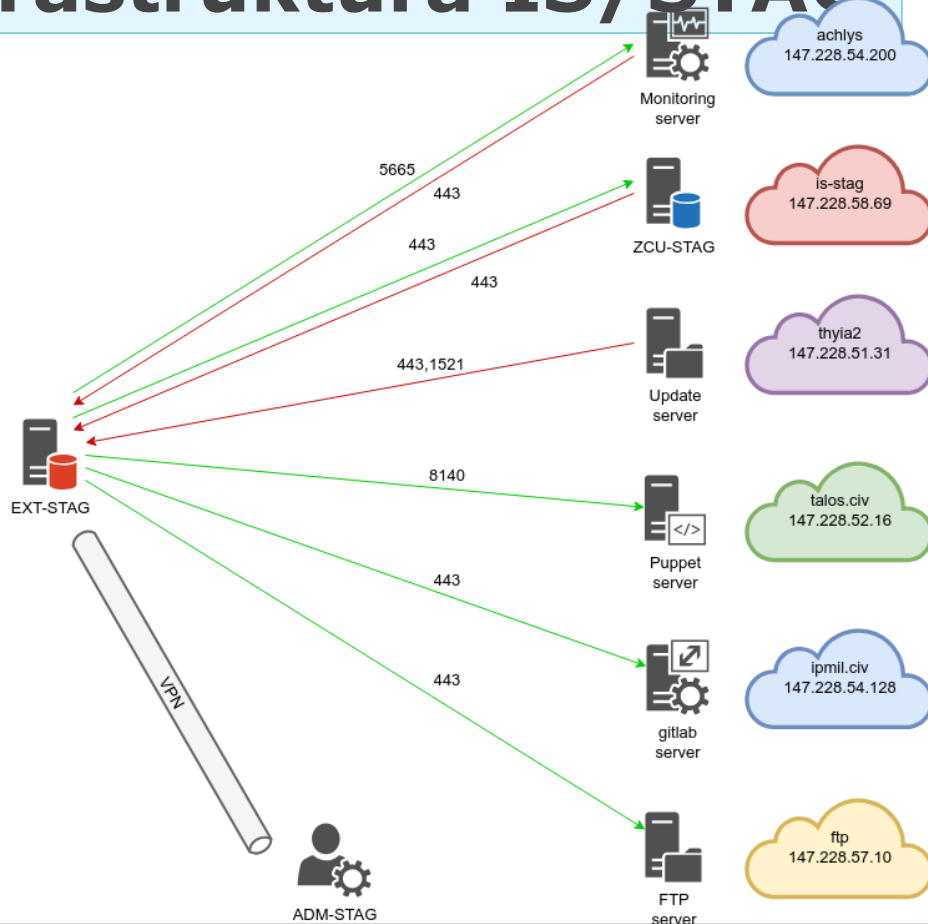
5. 5. 2026, Klasifikace: Veřejné, Autor: OSI CIV (Ing. Martin Šimek, PhD.)

Klasické začlenění IS/STAG do zákaznické infrastruktury

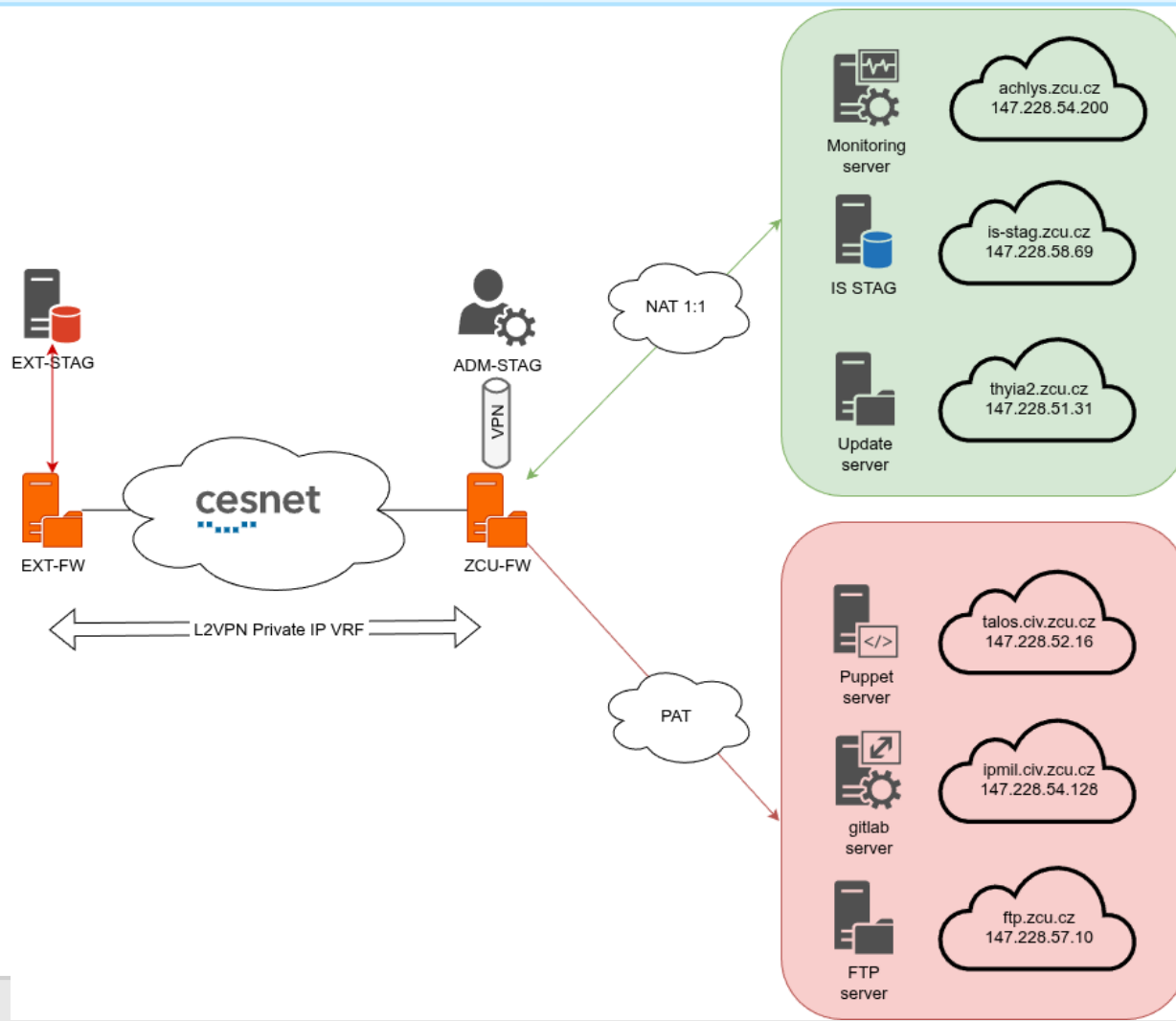
- Dokument <https://is-stag.zcu.cz/administratori/web/platforma/integrace.html>
 - Nutné nastavení firewallu na perimetru zákaznické sítě
 - Veškerá komunikace je šifrovaná na aplikační úrovni
 - dostatečná ochrana dat
- Technické požadavky ZKB na VIS jsou splněny
- Zákaznická analýza rizik může dát odlišné výsledky
 - Nutno řešit individuálně
- Přístupy administrátorů řešeny individuálním způsobem <https://is-stag.zcu.cz/administratori/databaze/vyvojari-adresy.html>
 - Zákazník řeší na své úrovni
 - Individuální přístup do zákaznické sítě
 - Plná kontrola nad přístupy na straně zákazníka

Komunikační infrastruktura IS/STAG

- Komunikace směrem ven
- Komunikace směrem dovnitř
- Omezení na konkrétní IP adresy
 - Na perimetru
 - Na serveru
- Plná kontrola nad datovými toky
- Plná kontrola nad přístupy administrátorů
 - Přímé nebo VPN
 - VPN... Různé systémy různé ověření (au)



- Privátní spojení mezi zákazníkem a ZČU
- Veškerá administrativní komunikace prochází pouze privátní sítí
- Nasazení nových verzí IS/STAG
- Automatizace a monitoring IS/STAG
- Jednotný VPN přístup administrátorů
- Realizace spojení prostřednictvím sítě CESNET
- Připojení do privátní sítě podobné připojení k CMS/KIVS, ale jednodušší
- Další interface/VLAN na perimetru zákaznické sítě
- Další interface/VLAN na serveru



Migrace na BKI IS/STAG

- Kontaktovat ZČU IS/STAG (RT)
 - Přidat kontakt na správce sítě
 - Kontakt na správce serverů
- Domluva na předávacím rozhraní s CESNET
 - Interface, VLAN
- Domluva IP adresního rozsahu BKI STAG
- Zprovoznění L2VPN mezi EXT-FW a ZCU-FW
 - EXT-FW není nutný, lze použít předávanou VLAN
- Přechod na BKI STAG
 - Konfigurace interface na konkrétních serverech

Konec, shrnutí a obrázek

- Na podzim 2025 jsme na ZČU absolvovali audit KB
- Podklady pro váš audit KB
- Zkušenosti z našeho auditu
- Zabezpečené přístupy

