ČZU
ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Odbor informačních a komunikačních technologií
Středisko infrastruktury
vedoucí Ing. Ladislav Stach
Kamýcká 129, 165 00 Praha 6 – Suchdol
Tel.: +420 224 38 6377, E-mail: stachl@oikt.czu.cz

Pravidla pro připojování zařízení a jejich užívání v sítích SCIENCE ČZU

Definice SCIENCE SÍTĚ ČZU

Odbor informačních a komunikačních technologií České zemědělské univerzity v Praze (dále jen OIKT) zřizuje a provozuje speciální typ datové počítačové sítě s označením SCIENCE ČZU.

Sítě SCIENCE ČZU jsou obecně určeny pro připojení koncových zařízení (PC, notebook…) a prvků síťové infrastruktury (dále jen IT zařízení), které nemůže OIKT spravovat centralizovaným způsobem nebo není vhodné z níže specifikovaných důvodů je připojovat do provozní počítačové sítě ČZU a současně u nich existuje odůvodněný požadavek na provoz v rámci IT infrastruktury ČZU.

Kategorie IT zařízení vhodných pro připojení do Science sítě ČZU:

- Servery nebo PC stanice pro speciální vědecké účely, které jsou v majetku třetích stran
- Vědecká IT zařízení, která jsou plně spravována na základě platné servisní smlouvy třetí stranou
- Vědecká IT zařízení v majetku ČZU pracující s jiným OS než MS Windows, jsou využívaná pro konkrétní vědecko-výzkumný projekt a neumožňující využít služby Active Directory z domény CZU.CZ

IT zařízení, které neodpovídá žádné z výše uvedených kategorií musí být připojeno pouze do prostředí provozní sítě ČZU a budou na něm aplikována bezpečnostní pravidla 802.1X, používaných na ČZU.

Jak připojit IT zařízení do sítě SCIENCE ČZU

IT zařízení je do sítě SCIENCE ČZU připojeno na základě požadavku potvrzeného vedoucím příslušného pracoviště/střediska, které bude IT zařízení provozovat. Žádost o připojení IT zařízení do SCIENCE ČZU je nutné zaslat aplikací Helpdesk.

Vedoucí OIKT si vyhrazuje právo žádost zamítnout v případě, že by požadované připojení IT zařízení mohlo způsobit problémy ve fungování celé datové sítě ČZU. V tomto případě bude vedoucí OIKT nebo pověřený pracovník OIKT neprodleně kontaktovat žadatele a pokusí se navrhnout náhradní řešení.

Pro každé připojené IT zařízení musí být jednoznačně definována odpovědná osoba z řad zaměstnanců ČZU (dále jen vlastník) a vedoucí příslušného pracoviště/střediska odpovídá za aktualizaci této osoby v případě, že dotyčný pracovník rozváže pracovní poměr s ČZU.

ČZU
ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Odbor informačních a komunikačních technologií
Středisko infrastruktury
vedoucí Ing. Ladislav Stach
Kamýcká 129, 165 00 Praha 6 – Suchdol
Tel.: +420 224 38 6377, E-mail: stachl@oikt.czu.cz

Zásady provozu IT zařízení v SCIENCE SÍTI ČZU

- IT zařízení jsou plně spravována a administrována vlastníkem a ten nese plnou odpovědnost za provoz tohoto IT zařízení

- OIKT poskytuje na dohodnutém rozhraní vybrané síťové služby (viz níže Přehled poskytovaných služeb pro síť SCIENCE ČZU) dle specifikace a tyto služby jsou dodávány v kvalitě odpovídající servisním smlouvám, které má uzavřené OIKT s dodavateli ČZU

- OIKT nenese žádnou odpovědnost za škody vzniklé na IT zařízení připojené do SCIENCE ČZU sítě nebo jeho provozem, ztrátu dat apod. OIKT nezajišťuje připojení těchto IT zařízení do systému Centrálního zálohování a archivace dat.

  Identifikační jména koncových IT zařízení musí splňovat jmennou konvenci ve tvaru „ČZU login vlastníka-SN-XX“, kde XX je identifikační číslo IT zařízení (např. NOVAK-SN-01). Povolenými znaky jsou písmena, číslice a znak „-“. Dodržení této jmenné konvence je klíčové pro správnou funkci DNS služeb a odpovídá jejich implementaci v síti ČZU.

- IT zařízení musí mít v každém okamžiku jasně definovaného vlastníka, který je aktivním zaměstnancem ČZU.

- OIKT poskytne potřebnou součinnost, pokud se třetí strana servisně stará o danné IT zařízení, ale s vyjímkou poskytovaných služeb (viz níže Přehled poskytovaných služeb pro síť SCIENCE ČZU) negarantuje reakční dobu na řešení provozních incidentů na IT zařízeních v Science síti ČZU.

- V případě, že se jedná o IT zařízení, které je majetkem ČZU si OIKT vyhrazuje právo na instalaci inventarizačního nástroje (pouze pro účely sw auditu a fyzické inventarizace IT zařízení). Instalace bude vždy prováděna po dohodě s vlastníkem. Vlastník IT zařízení je na žádost pracovníka OIKT povinen poskytnout potřebnou součinnost s pracovníky OIKT v rámci softwarového či hardwarového auditu.

- Pokud IT zařízení vykazuje znaky bezpečnostních hrozeb, OIKT si vyhrazuje právo omezit na dobu nezbytně nutnou přístup ke službám poskytovaným v SCIENCE ČZU síti, tj. de-facto zamezit přístup k datové síti ČZU. OIKT musí o

Odbor informačních a komunikačních technologií
Středisko infrastruktury
vedoucí Ing. Ladislav Stach
Kamýcká 129, 165 00 Praha 6 – Suchdol
Tel.: +420 224 38 6377, E-mail: stachl@oikt.czu.cz

této události informovat vlastníka obratem a upřesnit další kroky, které povedou k obnovení normálního provozu IT zařízení v SCIENCE ČZU síti.

Přehled poskytovaných služeb pro síť SCIENCE ČZU

Sítě SCIENCE ČZU jsou navrhovány jako vnitřní izolovaný prostor pro každou fakultu, či logický celek (např. rektorátní pracoviště). Vzájemná izolovanost je navržena z důvodu zabezpečení celé datové sítě ČZU proti proniknutí z neznámých zařízení a izolování případného ohrožení na jeden segment SCIENCE SÍTÍ ČZU. Tento izolovaný prostor obsahuje výjimky pro doplňkové služby, jako jsou např. služba DNS (pouze dotazování), e-mail či síťový tisk.

Výčet služeb v síti SCIENCE ČZU

1) přístup do celosvětové sítě internet se zapnutou ochranou IPS a SSL/TLS inspekcí na hraničním prvku (IPS zajišťuje preventivní ochranu proti útokům zvenku a SSL/TLS inspekce zabraňuje komunikaci se servery, které nepoužívají důvěryhodné certifikáty – nedůvěryhodné certifikáty mohou být expirované nebo podvržené), součástí ochrany jsou také logovací a monitorovací nástroje,

2) využívání interních a externích DNS serverů univerzity (ICMP, DNS – pouze dotazování),

3) přístup do sítě tiskáren dané fakulty (ICMP, TCP – 9100, UDP - 137, 161, 623). Síťový přístup na tiskárny dané fakulty či logického celku je ze sítě SCIENCE ČZU povolen,

4) přístup na poštovní služby univerzity:
   a. služby odesílání přes smtp.czu.cz : SMTPS (587, jen autentizovaně STARTLS, návod v https://helpdesk.czu.cz, sekce Znalostní databáze / Návody a postupy / Přístup k mailovým službám ČZU pro zaměstnance a doktorandy). Relay není ze science sítí povolen.
   b. služby Novell Groupwise: GWAVA karanténa (49385)
   c. služby Exchange na email.czu.cz : ICMP, OWA (HTTPS)
5) inventarizace LanDesk: TCP 5007 – směr server, TCP 9595 a UDP 38293 oba směry

Žádost o změnu služeb čerpaných v síti SCIENCE ČZU podává vlastník IT zařízení v systému Helpdesk, OIKT zajistí zdokumentování provedené úpravy a aktualizaci technických parametrů v provozní dokumentaci. Vedoucí OIKT si vyhrazuje právo žádost o změnu služby zamítnout v případě, že by požadovaná změna mohla způsobit problémy ve fungování celé datové sítě ČZU. V tomto případě bude vedoucí OIKT nebo pověřený pracovník OIKT neprodleně kontaktovat žadatele a pokusí se navrhnout náhradní řešení.

ČZU
ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Odbor informačních a komunikačních technologií
Středisko infrastruktury
vedoucí Ing. Ladislav Stach
Kamýcká 129, 165 00 Praha 6 – Suchdol
Tel.: +420 224 38 6377, E-mail: stachl@oikt.czu.cz

Fyzické umístění IT zařízení

Provozní prostory si pro IT zařízení připojené do SCIENCE ČZU sítě zajišťuje jeho vlastník sám. OIKT dle svých možností poskytne prostor centrální rozvodny/serverovny v objektech ČZU.

Servisní odstávky IT infrastruktury ČZU (schválený harmonogram)

IT zařízení připojená v síti SCIENCE ČZU se podřizují harmonogramu plánovaných servisních odstávek OIKT (viz harmonogram na https://www.oikt.czu.cz/, sekce odstávky). V plánovaných odstávkových termínech mohou být některé služby sítě SCIENCE ČZU nedostupné včetně dodávky elektrické energie a chlazení v centrální rozvodně/serverovně.

Seznam příloh:

1. Přehled povolených prostupů ze sítě SCIENCE ČZU
2. Žádost o připojení IT zařízení do sítě SCIENCE ČZU

ČZU
ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Odbor informačních a komunikačních technologií
Středisko infrastruktury
vedoucí Ing. Ladislav Stach
Kamýcká 129, 165 00 Praha 6 – Suchdol
Tel.: +420 224 38 6377, E-mail: stachl@oikt.czu.cz

Příloha č. 1 – Přehled povolených prostupů ze sítě SCIENCE ČZU

FW pravidla pro SCIENCE ČZU sítě						
Zdroj	**Cíl**	**Protokoly**	**Logování**	**IPS**	**SSL**	**Antivirus**
Všechny science sítě	smtp.czu.cz	ICMP, SMTP 587	ano	ano	ne	ne
Všechny science sítě	cv.czu.cz	ICMP, HTTP, HTTPS	ano	ano	ano	ne
Všechny science sítě	intranet.czu.cz	ICMP, HTTP, HTTPs	ano	ano	ano	ne
Všechny science sítě	(Novell_Groupwise) mail.rektorat.czu.cz mail.pef.czu.cz mail.fle.czu.cz mail.oikt.czu.cz mail.tf.czu.cz mail.af.czu.cz	TCP 49385	ano	ano	ne	ne
Všechny science sítě	Tiskárnové sítě (dle příslušnosti fakulty)	ICMP, TCP - 9100, UDP - 137, 161, 623	ano	ne	ne	ne
Všechny science sítě	Vnější DMZ	ICMP, HTTP, HTTPS	ano	ano	ano	ano
Všechny science sítě	Vnitřní DMZ	ICMP, HTTP, HTTPs	ano	ano	ano	ano
Všechny science sítě	connect.czu.cz	ICMP, rtmp	ano	ne	ne	ne
Všechny science sítě	ldms.czu.cz landesk.czu.cz	TCP – 5007, 9595 UDP - 38293	ano	ano	ne	ne
Všechny science sítě	Interní a externí DNS servery	ICMP, DNS	ne	ano	ne	ne
Všechny science sítě	Kitlab a Kixx	KIT	ano	ne	ne	ne
Všechny science sítě	Prostup do internetu	bez omezení	ano	ano	ano	ne
Všechny science sítě	Vnější služby ČZU	jako z internetu	ano	ano	ano	ne

Poznámka: služby GroupWise budou poskytovány jen do doby ukončení projektu migrace ČZU do prostředí Microsoft.