



Enterprise Computing Solutions - Education Services

## NABÍDKA ŠKOLENÍ

---

**Prosím kontaktujte nás zde**

Arrow ECS, a.s., 28. října 3390/111a, 702 00 Ostrava

Email: [training.ecs.cz@arrow.com](mailto:training.ecs.cz@arrow.com)  
Phone: +420 597 488 811



## Jemný úvod do SSL/TLS

<b>Kód:</b>	<b>DÉLKA:</b>	<b>CENA:</b>
OTH_CRYPT_SSL/TSL	24 Hours (3 DENNÍ)	Kč bez DPH 22,500.00

### Description

Pro zajištění důvěrnosti a autenticity přenášených informací se v prostředí internetu nejčastěji používá termín SSL/TLS. Jedná se o vrstvu zajišťující kryptografickou ochranu (tedy šifrování a detekci změny dat). Vzhledem k legislativě a obecnému vývoji kladoucímu důraz na soukromí se toto školení věnuje vysvětlení vztahů tak, aby bylo možné chránit informace společnosti a zákazníků. Zároveň nastiňuje vztahy k evropským nařízením (GDPR, eIDAS), zákonům (kybernetický zákon) a používaným oborovým normám.

### Cíle

- Seznámení s vývojem a architekturou SSL/TLS
- Vysvětlení omezení jednotlivých ciphersuit
- Obeznamení se základními útoky a příčinou existujících slabín
- Vysvětlení práce s certifikáty a certifikačními autoritami
- Obeznamení se s nařízením eIDAS
- Minimální právní základ, přehled zákonů a norem jako limitující podmínkou pro hardening

### Určeno pro

Kurz je určen pro správce IT věnující se bezpečnosti, správce systémů, dále pak pro síťové a bezpečnostní konzultanty. Je koncipován tak, aby jim umožnil orientaci v problematice a poskytl základní informace, jak bezpečně nastavit parametry pro splnění povinností kladených normami.

### Vstupní znalosti

Účastník by měl mít zkušenosti se správou systémů, základní přehled o počítačové bezpečnosti a základní představu o fungování sady protokolů TCP/IP.

### Program

Základní termíny a uvedení do problematiky  
Architektura SSL/TLS  
Historie a vývoj, podpora ciphersuites v jednotlivých verzích  
Zhodnocení bezpečnosti ciphersuites  
Protokoly pro výměnu klíčů  
Útoky na kryptografii v SSL/TLS  
Verze SSL/TLS  
Standardy a národní normy, zákony a jejich vztah k nařízením EU  
Podporované algoritmy, jejich opora v zákonech, nařízeních a normách  
Hardening  
Prostředí Java a Microsoft  
Webové servery: Apache, IIS, Lighthttpd, NGINX, Tomcat, WinHTTP  
Poštovní servery: Dovecot, Exchange, Postfix, Sendmail  
Databázové servery: MySQL/MariaDB, MongoDB, Postgress, SQLite  
VPN (OpenVPN)  
SSH  
Inspekce SSL  
Využití certifikátů  
CA, PKI a služby zajištění důvěry v prostředí elektronické komunikace  
Provozní vlastnosti  
Standardy ASN.1, OID a kódování Base64  
Formáty CER, DER, BER a uložení klíčů ve formátu PK7, PK12  
Certifikát a jeho struktura  
Důležité a volitelné parametry  
Normy rozšiřující vlastnosti certifikátů  
Vysvětlení metod kontroly platnosti certifikátů (path validation, CRL, OCSP)  
Křížové certifikáty a křížová certifikace autorit  
eIDAS

## Termíny školení

Termíny školení na vyžádání, [kontaktujte nás prosím](#)

## Dodatečné informace

Školení je možné zajistit na míru. [Kontaktujte nás pro bližší informace.](#)