TATE International, s.r.o.,
vydavatel časopisu DSM – data security management

p o ř á d á

Akademii ICT managementu

akademie ICT managementu

Bezpečné zdravotnictví

„Kyberbezpečnost jako součást moderní nemocnice“

Kurz:

Proč jít na kurz?

- Chcete být připraveni na NIS2?
- Víte co Vás čeká od noveho Zákona o kybernetické bezpečnosti?
- Jste členy vedení nemocnice anebo zdravotnického zařízení?
- Jste zřizovatelem nemocnice či jiných zdravotnických zařízení?
- Tento jednodenní vstup do podstatných oblastí informační bezpečnostise zaměřením na praktické zkušenosti umožní poznat základní prvky kyberbezpečnosti, jednotlivé vazby, zákonné zodpovědnosti a připravit se na přicházející regulaci bezpečnosti NIS2

Kurz je určen pro:

- Management nemocnic a zdravotnických zařízení
- Vedoucí lékaře
- Osoby zodpovědné za chod nemocnic, zřizovatelé, majitelé, členové představenstva, ředitelství zdravotnických zařízení

Získání certifikátu

- Po absolvování kurzu získáte kredity pro získání certifikátu „Certifikovaný Manager ICT“ (Certified Manager of ICT – CMICT).

NEJBLIŽŠÍ KURZY

DevOps – „Kdo chvíli stál, stojí opodál.”

Strategie ICT v 21. století II.
„Budování hodnoty ICT – lidé a peníze“

Digitální transformace
„Vítejte v džungli digitální transformace – nástroje a metody“

DIGITÁLNÍ SLUŽBY
v moderním světě a specifika průkaznosti

Umění řízení služeb
aneb SLA v praxi – „Důvěřuj, ale prověřuj“

KYBERBEZPEČNOST
„Povinnost ze zákona – dobrá pro všechny“

Proč Akademie ICT managementu?

Pozice ICT manažera se stává stále náročnější. Základní rozpor spočívá v požadované dvojroli. Na jedné straně se od CIO (Chief Information Officer) očekává schopnost komunikovat s vrcholovým managementem a obchodními jednotkami o podpoře a realizaci strategických cílů (ICT enablement and alignment), na druhé straně statutární orgány předpokládají, že CIO je manažer orientovaný na efektivní řízení ICT provozní továrny (ICT management and control). Kombinace těchto dvou požadavků klade na CIO v moderní společnosti nebývalé nároky. Po mnoha letech strávených v ICT oblasti a nejen v ní se skupina sdružená kolem TATE International a časopisu Data Security Management rozhodla usnadnit současnému CIO plnění jeho dvojrole systémem vzdělávacích kurzů vycházejících z dlouholeté světové i lokální praxe.

Bezpečné zdravotnictví „Kyberbezpečnost jako součást moderní nemocnice“

Počet kreditů: **8**

08:45–09:00	**Registrace účastníků**
09:00–09:30	**Úvod do IT** Trendy IT podporují jak rozvoj společností, tak oblasti kyberkriminality. Ukážeme si, jaké výhody a rizika jsou s vývojem spojená. Vysvětlíme si, kdo se snaží kyberútoky využít, jak probíhají, na koho cílí a jak budovat obranu. ■ Postavení IT a bezpečnosti ve společnosti ■ Trendy IT - Technologické výhody, Rizika ■ Kyberkriminalita, Kyberútoky a exponované osoby ■ Budování Kyberobrany ■ Kvíz
09:30–10:30	**Bezpečnostní dopady ve zdravotnictví** Jak moc je nemocnice na IT závislá a co se může stát, když by přestalo částečně či zcela IT fungovat? ■ Jste připraveni na to, co se může stát, když vypadne IT? ■ Jste schopni bez fungujícího IT poskytovat pacientům péči? ■ Může vás ohrozit zdravotechnika? ■ Lze se na to připravit? A kdo za to všechno bude odpovědný?
10:30–10:45	**Přestávka na kávu**
10:45–11:45	**Právní okénko pro statutáry ve zdravotnictví: Kyberbezpečnost – právní minimum** ■ Faktický stav – rizika v oblasti kybernetické bezpečnosti, možné negativní následky ■ Obecné povinnosti člena statutárního orgánu ■ Zvláštní povinnosti člena statutárního orgánu dle relevantních právních předpisů - zákon o zdravotních službách, ZKB, eIDAS, GDPR + ZoZOÚ, NIS2 ■ Zákon o kybernetické bezpečnosti – struktura, obsah, účinnost, povinnosti uložené společnosti a managementu, možné sankce, aktuality ■ Ochrana osobních údajů ■ Odpovědnost členů statutárních orgánů za porušení povinností, vč. trestní odpovědnosti, porovnání s odpovědností zaměstnance, vč. členů managementu ■ TOPO – trestní odpovědnost právnických osob ■ Připravovaný zákon o ochraně oznamovatelů – „whistleblowerů“ a jeho dopady na míru rizik a na odpovědnost statutárních orgánů
11:45–12:05	**Bezpečnostní killchain: Hrozby v kostce** Proti jakým protivníkům na kyberbojišti stojíte aneb hackerský svět v kostce… Praktická ukázka toho, jak postupuje útočník a čemu musí obránce zejména věnovat pozornost. Jakými mýty je opředena kyberbezpečnost a jejich společné boření. ■ Organizovaný zločin (zejména ransomware) – kdo to je, modus operandi, důsledky, platba výkupného, kryptoměny ■ Státní aktéři - kdo to je, modus operandi, důsledky ■ Threat intel, tradecraft a jeho pochopení pro řízení hrozeb ■ Medical OT, IoT, wearables - co to je a rizika s tím spojená
12:05–12:45	**Přestávka na oběd**
12:45–13:25	**Bezpečnostní killchain: Útok a obrana – praktická ukázka** ■ Killchain útoku ve virtuálním prostředí – co se děje, když jste pod útokem ■ Bezpečnostní minimum pro obranu před útočníkem (prevence, detekce, reakce, obnova) ■ Nejčastější chyby a mýty při nastavení obrany před útočníkem

Bezpečné zdravotnictví „Kyberbezpečnost jako součást moderní nemocnice“

Počet kreditů: **8**

13:25–14:25	**Ideální IT v nemocnici** Jak se dá definovat ideální IT? Je ideální IT právě to bezpečné? Existuje realizace konkrétní agendy, která je díky informačním technologiím efektivnější? Co pro ideální IT aktuálně zlepšit? Jak bude vypadat nemocniční IT v roce 2050. ■ Pracovní IT prostředí a denní agenda ■ Uživatelé vs. IT ■ Úskalí informačních systémů a aplikací a technologická zlomyslnost ■ Bezpečnostní omezení v IT prostředí ■ IT služby, požadavky, uživatelé a příběhy z praxe ■ Ochrana dat, GDPR a zdravý rozum ■ Profesní IT vs. „soukromé“ IT ■ Práce vs. zábava s technologiemi a zohlednění rizik ■ Dostupnost, kvalita a efektivita při využití běžných IT technologií ■ Bezpečnost ■ Jak na zajištění bezpečí ■ Eliminace rizik ■ Edukace, edukace, edukace ■ Ideální IT ■ Aktuální stav ■ Technologické možnosti ■ Nemocnice 2050
14:25–14:35	**Přestávka na kávu**
14:35–15:00	**Gamifikace formou CyberArena/Virtuální realita útoku** ■ Úniková hra ve virtuální realitě zaměřená na kyberbezpečnost. Zaměření je především na management a koncové uživatelé. Tato hra ukazuje pohled útočníka na zranitelné body organizace v různých scénářích. Je možné sehrát v soutěžním režimu „na body“, lze si vyzkoušet i o přestávce případně po skončení hlavního programu.
15:00–15:05	**Závěr kurzu**

LEKTOŘI

Petr Foltýn

Aktuálně působí jako náměstek ředitele pro IT ve Fakultním nemocnici Ostrava. V oblasti IT služeb a související bezpečnosti působí již více než 20 let a má rozsáhlé zkušenosti v oblasti komplexních integrací digitalizačních projektů. Působil v manažerských pozicích jak soukromé tak státní sféře v oblastech školství a zdravotnictví, kde mimo revizi interních procesů a tvorby strategií byl garantem implementací zásadních projektů pro zajištění kybernetické bezpečnosti a informačních systémů základní služby.

Tomáš Iránek

V současnosti působí jako manažer kybernetické bezpečnosti v Uherskohradišťské nemocnici. V IT se pohybuje více než 20 let, kde působil na různých pozicích od řadového programátora, přes manažera mezinárodního supportního týmu až po náměstka ředitele a to jak v komerčním sektoru, tak v poslední době ve zdravotnictví. V nedávné minulosti působil jako náměstek ředitele pro IT v Krajské nemocnici T. Bati ve Zlíně a nebo ve Fakultní nemocnici Brno.

Lukáš Klášterský

Působí v oblasti IT Infrastruktury. Za více než 20 let působení v oblasti IT a telekomunikací má bohaté zkušenosti s poskytováním ICT služeb, realizací projektů a transformací s přesahy do oblasti digitalizace a bezpečnosti, expertní znalosti ICT trendů. Působil na manažerských pozicích Lucent technologies, Telefonica O2, Česká pojišťovna/Generali Group.

Miroslav Uřičář

Advokát a partner LEGALITÉ advokátní kancelář, s. r. o., jednatel LEGALITÉ Data Protection Services s.r.o. Je členem Komise pro veřejné právo – komise pro správní právo Legislativní rady vlády ČR, členem Rozkladové komise ERÚ a rozhodcem Rozhodčího soudu při HK ČR a AK ČR. V letech 1999–2016 působil v top-manažerských pozicích u jednoho z největších operátorů elektronických komunikací, od roku 2004 jako ředitel útvaru práva, regulace, bezpečnosti a vnějších vztahů. Je vedoucím spoluautorem komentáře k GDPR v nakladatelství C.H.Beck.

Michal Wojnar

Je manažerem v oddělení Řízení rizik v pražské kanceláři PwC s několikaletou zkušeností s projekty v oblasti IT bezpečnosti, specializuje se na oblast IT rizik a IT bezpečnosti, auditní revize firemních procesů, interních kontrol a prověrky informačních systémů IT General Controls. Spoluzakladatel PwC Business Continuity fóra v ČR, je certifikovaným lektorem Game of Threats™.

Bezpečné zdravotnictví „Kyberbezpečnost jako součást moderní nemocnice“

P Ř I H L Á Š K A

Bezpečné zdravotnictví

akademie ICT managementu

Společnost: Oblast podnikání:

Adresa: PSČ: Město:

IČ: DIČ:

Jméno: Příjmení: Titul:

Funkce: Telefon: Fax:

E-mail: Předplatitel DSM: ne ❑ ano ❑ č. předplatitele:

Zúčastním se: kurzu ❑ workshopu ❑ Zálohovou fakturu: ne ❑ ano ❑

Účastnický poplatek ve výši Kč včetně DPH prosím uhraďte na účet TATE International, s.r.o. číslo **574171183/0300** u ČSOB a.s. Praha 1, IČ: 25148125, DIČ: CZ25148125.
Variabilní symbol: IČ firmy (soukromá osoba uvede číslo 9999).
Všechny bankovní poplatky spojené s registrací hradí účastník.

Dne: Podpis: Razítko:

Vyplněnou přihlášku zašlete **na e-mail: aict@tate.cz** nebo využijte možnosti **registrace na www.tate.cz.**

Akademii ICT managementu pořádá TATE International, s.r.o.,
vydavatel časopisu DSM - data security management, Hořejší nábřeží 21, 150 00 Praha 5,
tel.: +420 257 920 319–20, e-mail: aict@tate.cz.

Informace a účastnický poplatek

Místo konání:

Cena kurzu včetně workshopu **11.990 Kč + DPH 21 %**

Délka kurzu je 8 hodin. Počet kreditů za tento kurz je 8.
Workshopy jsou součastí všech bloků.

Účastnický poplatek kurzu zahrnuje kompletní studijní materiály a malé občerstvení.
V případě přihlášení 3 dny předem se poplatek navyšuje o 1.000,- Kč.
TATE International, s.r.o. si vyhrazuje právo zrušit kurz, pokud se na něj přihlásí méně jak 6 účastníků. V tomto případě Vám budou vráceny všechny již zaplacené poplatky.

Storno poplatky:

do 15-ti dnů před termínem konání kurzu se účtuje storno poplatek 1.000,- Kč. Do 3 dnů před zahájením kurzu je storno poplatek 50 % z ceny kurzu. Později jsou storno poplatky 100 % z ceny kurzu.

Detaily placení:

Platit můžete bankovním převodem nebo zálohovou fakturou, kterou obdržíte na vyžádání.
Po obdržení platby na náš účet Vám vystavíme daňový doklad a zašleme potvrzení účasti. Všechny poplatky musí být uhrazené na účet organizátora nejpozději den před konáním kurzu.