AMENITDAYS 2026 7.–8. 10. 2026 NOVÝ JIČÍN

Konference AmenitDays 2026

Dovolujeme si Vás pozvat na expertní a prakticky orientovanou IT konferenci AmenitDays 2026 s mnoha přednáškami pod vedením profesionálů ve svém oboru.

AmenitDays 2026 je dvoudenní odborná IT konference zaměřená na aktuální témata z oblasti kybernetické bezpečnosti, správy IT infrastruktury, ochrany dat a moderních cloudových technologií. Účastníci se mohou těšit na prakticky orientované přednášky vedené zkušenými specialisty z oboru, kteří se ve své každodenní praxi věnují bezpečnosti Windows prostředí, Microsoft 365, identitám, detekci hrozeb, správě sítí i ochraně firemních dat.
Program konference nabídne nejen technické přednášky zaměřené na interní fungování bezpečnosti Windows, problematiku identit v Microsoft 365 nebo aktuální kybernetické hrozby cílené na české prostředí, ale také praktické zkušenosti z oblasti XDR/MDR řešení, EDR, SIEM, sociálního inženýrství či zabezpečení datových úložišť. Součástí programu budou rovněž témata zaměřená na nejčastější chyby při správě infrastruktury a reálné scénáře z praxe.
Konference je určena především pro IT administrátory, bezpečnostní specialisty, správce sítí, IT manažery, pracovníky odpovědné za kybernetickou bezpečnost i všechny odborníky, kteří chtějí získat přehled o současných bezpečnostních rizicích, moderních technologiích a osvědčených postupech z praxe. AmenitDays 2026 nabídne prostor nejen pro vzdělávání, ale také pro sdílení zkušeností a networking s odborníky z IT komunity.

AmenitDays 2026

Místo konání:
EDUCA - SOŠ, s. r. o.
Bohuslava Martinů 1994/4, 741 01 Nový Jičín
Parkování:
Parkoviště U Stadionu - 140 m, Parkoviště zimní stadion - 318 m

Informace najdete také na **www.AmenitDays.cz**.

Harmonogram přednášek:

1. den

Středa 7. 10. 2026
09:00 - 09:15 Registrace
09:15 - 10:00 | 1. přednáška | **Windows Security Internals**
10:00 - 10:15 | Přestávka
10:15 - 11:00 | 2. přednáška | **Microsoft 365 a identity jsou noční můra - část 1.**
11:00 - 11:15 | Přestávka
11:15 - 12:00 | 3. přednáška | **Jak se stát adminem (a proč je to pořád tak snadné)**
12:00 - 13:30 | Oběd
13:30 - 14:15 | 4. přednáška | **Tichý zloděj: Odhalení 18měsíční infiltrace infostealerem cíleným na Česko**
14:15 - 14:30 | Přestávka
14:30 - 15:15 | 5. přednáška | **Microsoft 365 a identity jsou noční můra - část 2.**
15:15 - 15:30 | Přestávka
15:30 - 16:15 | 6. přednáška | **IP kamera už není jen kamera: kybernetická bezpečnost fyzických bezpečnostních technologií v praxi IT**
2. den

Čtvrtek 8. 10. 2026
09:00 - 09:15 Registrace
09:15 - 10:00 | 1. přednáška | **ESET: XDR a MDR jako odpověď na ZoKB a AI hrozby**
10:00 - 10:15 | Přestávka
10:15 - 11:00 | 2. přednáška | **Ubiquiti UniFi – na co si dát pozor a nejčastější chyby v praxi**
11:00 - 11:15 | Přestávka
11:15 - 12:00 | 3. přednáška | **Veeam, bezpečnost dat – Windows versus Linux**
12:00 - 13:30 | Oběd
13:30 - 14:15 | 4. přednáška | **IPS, EDR, SIEM a UEBA aneb kolik akronymů vlastně potřebujeme pro zajištění bezpečnosti?**
14:15 - 14:30 | Přestávka
14:30 - 15:15 | 5. přednáška | **Sociální inženýrství aneb nejsnazší metoda hackingu**
15:15 - 15:30 | Přestávka
15:30 - 16:15 | 6. přednáška | **Synology – možnosti ochrany dat a přístupy, které dnes dávají smysl kombinovat**

Obsah přednášek:

1. den

1. přednáška
Windows Security Internals
Většina uživatelů (a bohužel i správců) končí u kontroly, zda v "Centru zabezpečení" svítí zelený přepínač. Ale co se skutečně stane v kernelu, když zapnete izolaci jádra? Proč vás Tamper Protection může zachránit před ransomwarem víc než samotný signaturový AV? V této přednášce rozebereme moderní bezpečnostní vrstvy Windows, které jsou často přehlížené nebo špatně pochopené. Podíváme se na Virtualization-Based Security (VBS), vysvětlíme si, jak Credential Guard brání extrakci hesel z paměti LSA, a proč jsou Attack Surface Reduction (ASR) pravidla tou nejlevnější a nejúčinnější cestou k hardeningu, o které nikdo nemluví.
Přednášející: ***Jan Marek***, Founder & Adversarial Tactics Trainer, falconea

2. přednáška
Microsoft 365 a identity jsou noční můra – část 1.
Identity jsou dnes nejčastějším cílem útoků – a zároveň největší slabinou většiny organizací. Stačí jeden kompromitovaný účet a útočník má otevřené dveře. Tato přednáška odhalí nejkritičtější bezpečnostní chyby ve správě identit v Microsoft 365, zejména v hybridním prostředí, a ukáže, jak jsou v praxi zneužívány. Ukážeme si klíčové pilíře zabezpečení identity. Přednáška bude obsahovat množství živých ukázek.
Přednášející: ***Lubomír Ošmera***, Microsoft Security trainer, konzultant a red teamer
|MCT|MCSE|CEI|CEH|CND|CCNA|CARTP|CAWASP|CRTE|CESP

3. přednáška
Jak se stát adminem (a proč je to pořád tak snadné)
Zapomeňte na "Unquoted Service Paths". V moderním on-prem prostředí, kde nás hlídá EDR a systém je plně opatchovaný, musíme jako testeři přemýšlet jinak. Tato přednáška je shrnutím mých "Notes from the Field" z posledních let, kdy k eskalaci oprávnění vedou i sofistikovanější cesty než jen zapomenuté heslo v konfiguračním souboru.
Přednášející: ***Jan Marek***, Founder & Adversarial Tactics Trainer, falconea

4. přednáška
Tichý zloděj: Odhalení 18měsíční infiltrace infostealerem cíleným na Česko
Infostealer malware cílený na Českou republiku zůstal v prostředí nemocnice neodhalen déle než 18 měsíců. Jak je možné, že takto dlouho unikal detekci? K jeho odhalení došlo až během implementace EDR řešení, která vedla k eskalaci aktivit útočníka. Malware na tuto situaci okamžitě reagoval pokusy o skrytí své činnosti, deaktivaci bezpečnostních nástrojů, vytvoření perzistence a urychlený exfil dat. Přednáška nabídne detailní rozbor celého incidentu. Od schopností infostealeru a rozsahu odcizených dat, přes netradiční způsoby komunikace s C&C servery, až po kompletní časovou osu útoku. Zaměří se také na reakci nemocničního IT týmu v průběhu incidentu.
Přednášející: ***David Pecl***, Security Consultant, Security Avengers

5. přednáška
Microsoft 365 a identity jsou noční můra - část 2.
Identity jsou dnes nejčastějším cílem útoků - a zároveň největší slabinou většiny organizací. Stačí jeden kompromitovaný účet a útočník má otevřené dveře. Tato přednáška odhalí nejkritičtější bezpečnostní chyby ve správě identit v Microsoft 365, zejména v hybridním prostředí, a ukáže, jak jsou v praxi zneužívány. Ukážeme si klíčové pilíře zabezpečení identity. Přednáška bude obsahovat množství živých ukázek.
Přednášející: ***Lubomír Ošmera***, Microsoft Security trainer, konzultant a red teamer |MCT|MCSE|CEI|CEH|CND|CCNA|CARTP|CAWASP|CRTE|CESP

6. přednáška
IP kamera už není jen kamera: kybernetická bezpečnost fyzických bezpečnostních technologií v praxi IT
Moderní IP kamery, interkomy, přístupové systémy, reproduktory nebo detektory už dávno nejsou izolované prvky fyzické bezpečnosti. Jsou to plnohodnotná síťová zařízení, která vstupují do stejného prostředí jako servery, pracovní stanice, identity, logování, SIEM, segmentace sítí nebo pravidla pro správu zranitelností. Přednáška prakticky ukáže, proč by fyzická bezpečnost měla být součástí kybernetické bezpečnosti organizace, jaká rizika vznikají při špatně navržených kamerových systémech a jak nad nimi přemýšlet z pohledu IT administrátora nebo security týmu. Zaměříme se na témata jako hardening zařízení, firmware management, správa identit a přístupů, certifikáty, 802.1X, šifrování, auditní stopa, logování do SIEM, segmentace sítě, bezpečný lifecycle management a dopady nových regulatorních požadavků typu NIS2, CER nebo Cyber Resilience Act. Cílem není marketingový pohled na kamerové systémy, ale praktické propojení světa fyzické bezpečnosti a kybernetické správy infrastruktury.
Přednášející: ***Mgr. Dalibor Smažinka, MBA, LLM***, Key Account Manager pro koncové zákazníky, Axis Communications

2. den

1. přednáška
ESET: XDR a MDR jako odpověď na ZoKB a AI hrozby
Jak detekovat kybernetický incident a včas na něj reagovat? Jak se postavit novým hrozbám spojeným s AI a jejím zneužitím? Odpovědí jsou novinky v XDR platformě ESET PROTECT. Novinky v platformě ESET PROTECT – vylepšení XDR a MDR, nová nativní ochrana cloudu, vylepšení ECOS, nový modul pro ochranu před zneužitím AI modelů a ESET Remote Access vzdálený přístup.
Přednášející: ***Ondřej Dědič***, Solution Architect, ESET software spol. s r.o.

2. přednáška
Ubiquiti UniFi – na co si dát pozor a nejčastější chyby v praxi
Z pohledu návrhu a provozu – typické chyby, špatná očekávání od UniFi, defaultní nastavení, limity platformy a doporučení, jak se jim vyhnout. Nejde o certifikační ani produktové školení, ale o praktický pohled vycházející z reálných nasazení.
Přednášející: ***Pavel Berry***, AI & Cloud Architect | Co-founder | Solution Engineer, PGNT

3. přednáška
Veeam, bezpečnost dat – Windows versus Linux
Obsah přednášky připravujeme...
Přednášející: ***Martin Kühpast***, IT konzultace a řešení, certifikovaný lektor

4. přednáška
Téma přednášky připravujeme...IPS, EDR, SIEM a UEBA, aneb kolik akronymů vlastně potřebujeme pro zajištění bezpečnosti?
Potřeba smysluplné identifikace bezpečnostních potřeb organizací a řízeného výběru bezpečnostních opatření, namísto „tupého“ kontinuálního pořizování dalších a dalších technologických platforem.
Přednášející: ***Jan Kopřiva***, Cyber Security Consultant & Trainer at Nettles Consulting

5. přednáška
Sociální inženýrství, aneb nejsnazší metoda hackingu
Jak postupuje hacker, pokud chce napadnout daný cíl, například banku? Začne prolamovat internetové bankovnictví, hraniční firewall či hesla služeb? Rozhodně může. Avšak chytrý hacker zvolí cestu nejmenšího odporu. Místo prolamování technických zabezpečení zacílí na nejslabší článek celého IT ekosystému - na člověka, na zaměstnance banky, na Vás. Na základě svojí mnohaleté praxe etického hackera představím konkrétní techniky, které kyberzločinci při tomto postupu, zvaném sociální inženýrství, používají.
Přednášející: ***Lukáš Antal***, CISSP, CEH, Ethical Hacker & Co-founder, TandemSec

6. přednáška
Synology – možnosti ochrany dat a přístupy, které dnes dává smysl kombinovat
Přehled nástrojů a produktových řad, které dnes Synology nabízí pro ochranu dat - od klasických NASů, snapshotů a Active Backup for Business až po novější přístupy typu ActiveProtect. Cílem je dát účastníkům koncepční přehled možností, nikoliv řešit konkrétní incidenty do hloubky.
Přednášející: ***Pavel Berry***, AI & Cloud Architect | Co-founder | Solution Engineer, PGNT