

Dovolujeme si Vás pozvat na expertní a prakticky orientovanou IT Konferenci AmenitDays 2023 s mnoha přednáškami pod vedením profesionálů ve svém oboru.

# AmenitDays 2023

## 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](http://www.AmenitDays.cz).

---

## Harmonogram přednášek:

### 1. den

**Středa 11. 10. 2023**

08:00 - 08:30 Registrace

08:30 - 09:30 | 1. přednáška | **Jak testovat připravenost na kybernetické útoky**

09:30 - 09:45 | Přestávka

09:45 - 10:45 | 2. přednáška | **Nákupy a získávání přihlašovacích údajů do společností**

10:45 - 11:00 | Přestávka

11:00 - 12:00 | 3. přednáška | **Zvýšení bezpečnosti koncových zařízení s využitím  
Virtualization Based Security ve Windows**

12:00 - 13:30 | Oběd

13:30 - 14:30 | 4. přednáška | **Hacktivismus, vydírání a špatná reputace s využitím DoS a  
DDoS**

14:30 - 14:45 | Přestávka

14:45 - 15:45 | 5. přednáška | **Jak hacker přemýšlí o vašem Microsoft 365, aneb má i u vás  
dveře otevřené?**

15:45 - 16:00 | Přestávka

16:00 - 17:00 | 6. přednáška | **Audit bezpečnosti Active Directory**

[Obsah přednášek prvního dne](#)

## 2. den

Čtvrtek 12. 10. 2023

08:00 - 08:30 Registrace

08:30 - 09:30 | 1. přednáška | **IOT v domácím prostředí více pod kontrolou / ESET Patch Management**

09:30 - 09:45 | Přestávka

09:45 - 10:45 | 2. přednáška | **NÚKIB s novinkami k evropské směrnici NIS2**

10:45 - 11:00 | Přestávka

11:00 - 12:00 | 3. přednáška | **Veeamem proti ransomware**

12:00 - 13:30 | Oběd

13:30 - 14:30 | 4. přednáška | **Umělá inteligence vs. autorské právo**

14:30 - 14:45 | Přestávka

14:45 - 15:45 | 5. přednáška | **Ukázka detekčních schopností u nezabezpečených protokolů Windows 1**

15:45 - 16:00 | Přestávka

16:00 - 17:00 | 6. přednáška | **Ukázka detekčních schopností u nezabezpečených protokolů Windows 2**

[Obsah přednášek druhého dne](#)

---

## Obsah přednášek:

### 1. den

#### 1. přednáška

##### **Jak testovat připravenost na kybernetické útoky**

Tato přednáška se zaměřuje na metody testování bezpečnosti organizace a hodnocení její připravenosti na kybernetické útoky. Budeme se zabývat otázkami, jako jsou: Jak správně testovat bezpečnost organizace? Jaká jsou nejlepší opatření pro případ kybernetického útoku? Jaké jsou nejnovější trendy a technologie v oblasti kybernetické bezpečnosti? Naším cílem je poskytnout ucelený přehled toho, jak měřit kvalitu bezpečnosti organizace a připravenost na kybernetické útoky, a poskytnout praktické tipy pro zlepšení zabezpečení informačních systémů.

Přednášející: **Marek Jan**, bezpečnostní konzultant a architekt s více než 15 lety osvědčených zkušeností, zaměřuje se především na produkty v oblasti kybernetické bezpečnosti, soukromého a veřejného cloudu

#### 2. přednáška

##### **Nákupy a získávání přihlašovacích údajů do společností**

Během této přednášky se zaměříme na postupy aktérů hrozeb ve vztahu k získávání přístupů do organizací. Vysvětlíme si, jak se aktéři hrozeb dostávají k přístupům a jak tyto informace mohou zneužít. Ukážeme si, jak obcházejí více-faktorové zabezpečení při přístupu k webovým aplikacím. Poskytneme vám ucelený pohled o problematice infostealerů a jejich využívání APT skupinami.

Přednášející: **Hejda Daniel**, konzultant a architekt řešení Microsoft Products, primární zaměření na spolupráci uživatelů v rámci organizace

#### 3. přednáška

##### **Zvýšení bezpečnosti koncových zařízení s využitím Virtualization Based Security ve Windows**

V této přednášce se zaměříme na koncept Virtualization Based Security ve Windows, který umožňuje izolovat kritické části operačního systému od aplikací a uživatelských dat, čímž se zvyšuje ochrana před útoky a zneužitím systému. Prozkoumáme, jak Virtualization Based Security funguje, jaké jsou jeho klíčové prvky a jaké výhody poskytuje v porovnání s tradičními bezpečnostními řešeními.

Přednášející: **Marek Jan**, bezpečnostní konzultant a architekt s více než 15 lety osvědčených zkušeností, zaměřuje se především na produkty v oblasti kybernetické bezpečnosti, soukromého a veřejného cloudu

## 4. přednáška

### Hacktivismus, vydírání a špatná reputace s využitím DoS a DDoS

O uskupení Anonymous jste jistě slyšeli a pravděpodobně i o skupině KILLNET. Pojďme se společně podívat, očima hackera, jak lze realizovat Denial of Service (DoS) a Distributed Denial of Service (DDoS). Ukážeme vám, na jaké části infrastruktury a webové aplikace je možné tento útok zacílit. Během přednášky vyčerpáme prostředky serveru a předvedeme si, jak lze útok realizovat proti skutečné infrastruktuře. V neposlední řadě vám ukážeme, jaké nástroje mohou aktéři hrozeb použít k monitoringu cíle a k monitoringu funkčnosti jejich kódu.

Přednášející: **Hejda Daniel**, konzultant a architekt řešení Microsoft Products, primární zaměření na spolupráci uživatelů v rámci organizace

## 5. přednáška

### Jak hacker přemýšlí o vašem Microsoft 365, aneb má i u vás dveře otevřené?

Typické scénáře útoku, časté prohřešky a k čemu to až může vést.

Přednášející: **Lubomír Ošmera**, CyberSecurity, Microsoft Cloud trainer and consultant (MCT, MCSE: Cloud platform and infrastructure, CEHv10, CND, CCNA, Microsoft 365 security certified)

## 6. přednáška

### Audit bezpečnosti Active Directory

Nejčastější nálezy u zákazníků - najdou se i u vás?

Přednášející: **Lubomír Ošmera**, CyberSecurity, Microsoft Cloud trainer and consultant (MCT, MCSE: Cloud platform and infrastructure, CEHv10, CND, CCNA, Microsoft 365 security certified)

## 2. den

### 1. přednáška

#### IOT v domácím prostředí více pod kontrolou

Řada incidentů ve světě IOT vede k myšlence, zda nelze tato zařízení provozovat trochu alternativně a nejlépe „mainstreamem“....

Přednášející: **Hák Igor**, odborník na viry, který pracuje u společnosti Eset téměř 20 let

#### ESET Patch Management

Přednáška na téma nové technologie od ESETU. Řešení pro správu zranitelností a záplat.

Přednášející: **Palička Radek**, zkušený a certifikovaný specialista na antivirové řešení

### 2. přednáška

#### NÚKIB s novinkami k evropské směrnici NIS2

Přiblížíme změny, které s sebou nese směrnice NIS2, koho se bude dotýkat a jakou podobu má její transpozice do českého právního řádu.

Přednášející: **Patrik Fráňa**, referent bezpečnosti státu, oddělení regulace soukromého sektoru, Národní úřad pro kybernetickou a informační bezpečnost

### 3. přednáška

#### Veeamem proti ransomware

...aneb jak využít technologie Veeam pro ochranu před napadením ransomware – přehled o nástrojích Veeam využitelných pro bezpečné uložení záloh dat, popis vhodné architektury řešení s ohledem na bezpečnost, seznam doporučených postupů pro minimalizaci možnosti ztráty dat.

Přednášející: **Martin Kühpast**, IT konzultace a řešení, certifikovaný lektor

### 4. přednáška

#### Umělá inteligence vs. autorské právo

Autorské právo k vytvořenému dílu za použití umělé inteligence. Nová regulace EU.

Přednášející: Bude zveřejněno později.

## **5. přednáška**

### **Ukázka detekčních schopností u nezabezpečených protokolů Windows 1**

Jak to vidí útočníci.

Přednášející: **Miloš Urbiš**, Lektor je soudní znalec v oboru kybernetika, odvětví výpočetní technika se specializací na bezpečnost informačních technologií. Konzultant pro kybernetickou bezpečnost. Jeho dosavadní praxe zaručuje kvalitu školení s předáváním praktických zkušeností.

## **6. přednáška**

### **Ukázka detekčních schopností u nezabezpečených protokolů Windows 2**

Jak jsme to schopni detekovat my. A co jsme schopni s tím udělat.

Přednášející: **Miloš Urbiš**, Lektor je soudní znalec v oboru kybernetika, odvětví výpočetní technika se specializací na bezpečnost informačních technologií. Konzultant pro kybernetickou bezpečnost. Jeho dosavadní praxe zaručuje kvalitu školení s předáváním praktických zkušeností.