



KYBERNETICKÁ
BEZPEČNOST



Projekt OPVK Vzdělávací modul Kybernetická bezpečnost

KYBERNETICKÁ BEZPEČNOST

Základní kurz kybernetické bezpečnosti



Seznam spolupracovníků:

Pavel Minařík

minarik@invea.cz

Lukáš Vondráček

vondracek@elat.cz

Petr Lacina

placina@uniscomp.cz

Petr Mikšovič

petr.miksovic@sovanet.cz

Petr Linke

petr.linke@novicom.cz

KYBERNETICKÁ BEZPEČNOST DOSTUPNÉ PROSTŘEDY A NÁSTROJE

1.1.1. SHRnutí

Technologií pro zajištění bezpečnosti datové infrastruktury je celá řada. Základní orientace v těchto technologiích a principech jejich fungování je klíčová pro zvládnutí procesu výběru adekvátních technických prostředků, jejich adaptaci a implementaci v prostředí podnikové IT infrastruktury.

Klíčové pojmy:

firewall, systém detekce průniků (IDS/IPS), antivirus, proxy, Unified Threat Management (UTM), řízení přístupu do sítě (NAC), kontrola privilegovaných účtů, monitorování výkonu aplikací, Security Information Event Management (SIEM), Security Operation Center (SOC).

Obsah podkapitoly:

- Přehled dostupných technických prostředků
- Dokumentace IS
- Identity management
- Firewall, IDS/IPS
- Antivirus
- Šifrování
- Provozní dohled
- Řízení přístupu do sítě
- Monitorování provozu
- Sledování aplikací
- Audit účtů
- Centrální log & SIEM
- Ochrana/prevence úniků dat

**PRÁVĚ PROHLÍŽÍTE DEMO VERZI VZDĚLÁVACÍHO MODULU
KYBERNETICKÁ BEZPEČNOST**

**V případě Vašeho zájmu vidět plnou verzi e-learningu nás prosím
kontaktujte na skoleni@nsmcluster.com**