

Aktivní bezpečnost sítě



Jindřich Šavel

27/11/2014

- **Představení společnosti**
- **Koncept aktivní bezpečnosti sítě**
- **Spolehlivé infrastruktura pro DDI/NAC řešení**

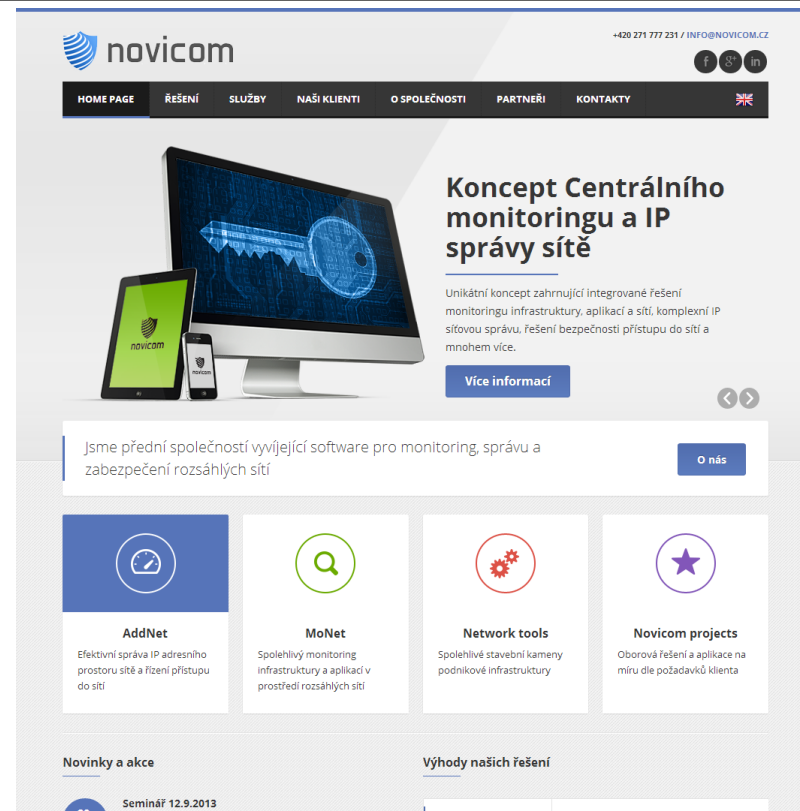
- Česká společnost zabývající se

- vývojem,
- dodávkami
- a provozem

systémů pro

- správu sítí
- monitoring
- bezpečnost
- a komunikace

- Orientace na střední a velké zákazníky a na dále na všechny vyžadující vysokou míru bezpečnosti a provozní spolehlivosti svých systémů
- Společnost s historií - 20 let českém trhu



MoNet

*Řešení distribuovaného monitoringu IT infrastruktury
a aplikací*

AddNet

*Efektivní a správa IP prostoru a bezpečnost přístupu v
rozsáhlých sítí*

Network tools

*Sada nástrojů pro vysoce efektivní a bezpečný provoz
IT infrastruktury*

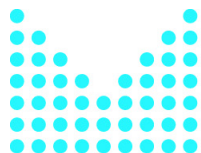
Projects

Oborová a customizovaná řešení

Novicom SGP – Secure Grid Platform

Novicom SDP – Secure Delivery Protocol

- **Novicom SGP (Secure Grid Platform)**
 - technologická platforma pro nadstandardní provozní spolehlivost Novicom systémů a jejich integrovaných klíčových služeb (L2/infrastrukturní monitoring a základní síťové služby DHCP/ DNS/ Radius)
 - vícenásobná redundance typu Active-Active, podpora hierarchického a distribuovaného modelu v prostředí rozsáhlých sítí
- **Novicom SDP (Secure Delivery Protocol)**
 - vlastní komunikační protokol navržený pro zajištění spolehlivé komunikace v prostředí velice nekvalitní sítě
 - pracuje na linkách s chybovostí až 95%
 - garance maximálního zabezpečení přenášených dat (military grade security)
- **Novicom FireBox platforma**
 - systém HW a virtuálních apliančí, zvyšující bezpečnost, spolehlivost a servisní flexibilitu pro klíčové komunikační a bezpečnostní funkce SGP
 - je založené na OS Linux s bezpečnostními úpravami kernelu, s nezávislými prvky centrální správy a zálohování/obnovy



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

 Univerzita Tomáše Bati ve Zlíně



Office DEPOT
Taking Care of Business



Ministerstvo obrany
České republiky

TOPTRANS

 **Česká pošta**

OSTRAVA!!!



 **ČESKÝ ROZHLAS**

AUTODÍLY  **AUTO ŠTANGL**



OBOROVÁ ZDRAVOTNÍ POJIŠŤOVNA
ZAMĚSTNANCŮ BANK, POJIŠŤOVEN
A STAVEBNICTVÍ


wüstenrot



- Koncept připravený na půdě NSMC
- **Network Security Monitoring Cluster**
 - *kooperační odvětvové uskupení zaměřené na oblast bezpečnosti počítačových sítí a bezpečnosti v ICT*
- **Aktivity klastru**
 - společné projekty
 - v oblasti technické infrastruktury inovačního charakteru,
 - aplikovaného výzkumu, vývoje a inovací
 - návrh a integrace komplexních řešení v oblasti monitorování bezpečnosti sítí
 - osvěta týkající se bezpečnosti počítačových sítí a informací, školení a vzdělávání
 - sdílení informací o aktuálních trendech v oblasti bezpečnosti sítí
 - návrhy úpravy právních norem v oblasti bezpečnosti ICT infrastruktury a jejího zabezpečení
 - komunikace s organizacemi a asociacemi zabývající se bezpečností počítačových sítí (např. ENISA, IT Security in Germany atd.)



www.kybernetickabezpecnost.eu

- Pro vedoucí pracovníky a management organizací

 **KYBERNETICKÁ
BEZPEČNOST**

Projekt CZ.1.07/3.2.04/05.0014: Vzdělávací modul Kybernetická bezpečnost.

KYBERNETICKÁ BEZPEČNOST V PODNIKU

VZDĚLÁVACÍ KURZ PRO VEDOUcí PRACOVNÍKY A MANAGEMENT,
ZEJMÉNA ŘEDITELE, FINANČNÍ ŘEDITELE A DALŠÍ DECISION MAKERY



Znáte úroveň zabezpečení Vaší firemní sítě?
Máte chráněná data? Víte, jak se chovají uživatelé?
Je transfer dat k vašim cloudovým službám bezpečný?
Jsou služby, které využíváte, v požadované kvalitě?
Bude nutná implementace řešení pro podporu
kybernetického zákona ve Vaše podniku/organizaci?

Pokud neznáte některou z odpovědí, je náš kurz určen pro Vás!



Absolvováním kurzu budete schopni

- :: lépe se orientovat v jednotlivých nástrojích ve firemní síti,
- :: identifikovat kritická místa v podniku,
- :: sestavit investiční plán pro nákup IT řešení,
- :: zavést opatření vedoucí k dlouhodobě udržitelné bezpečné síti a tedy i zvýšení konkurenceschopnosti



evropský
sociální
fond v ČR



EVROPSKÁ UNIE

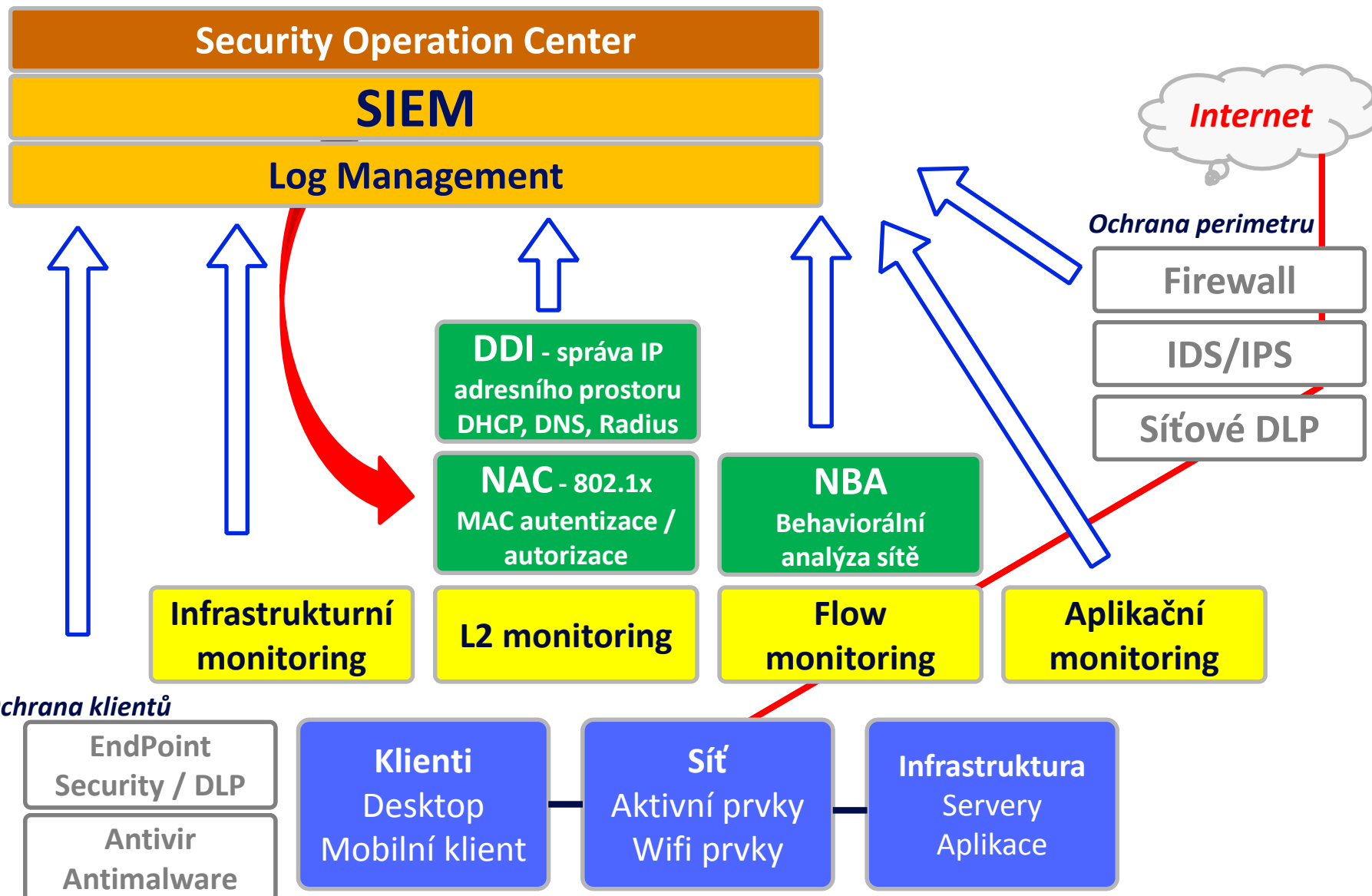


MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY

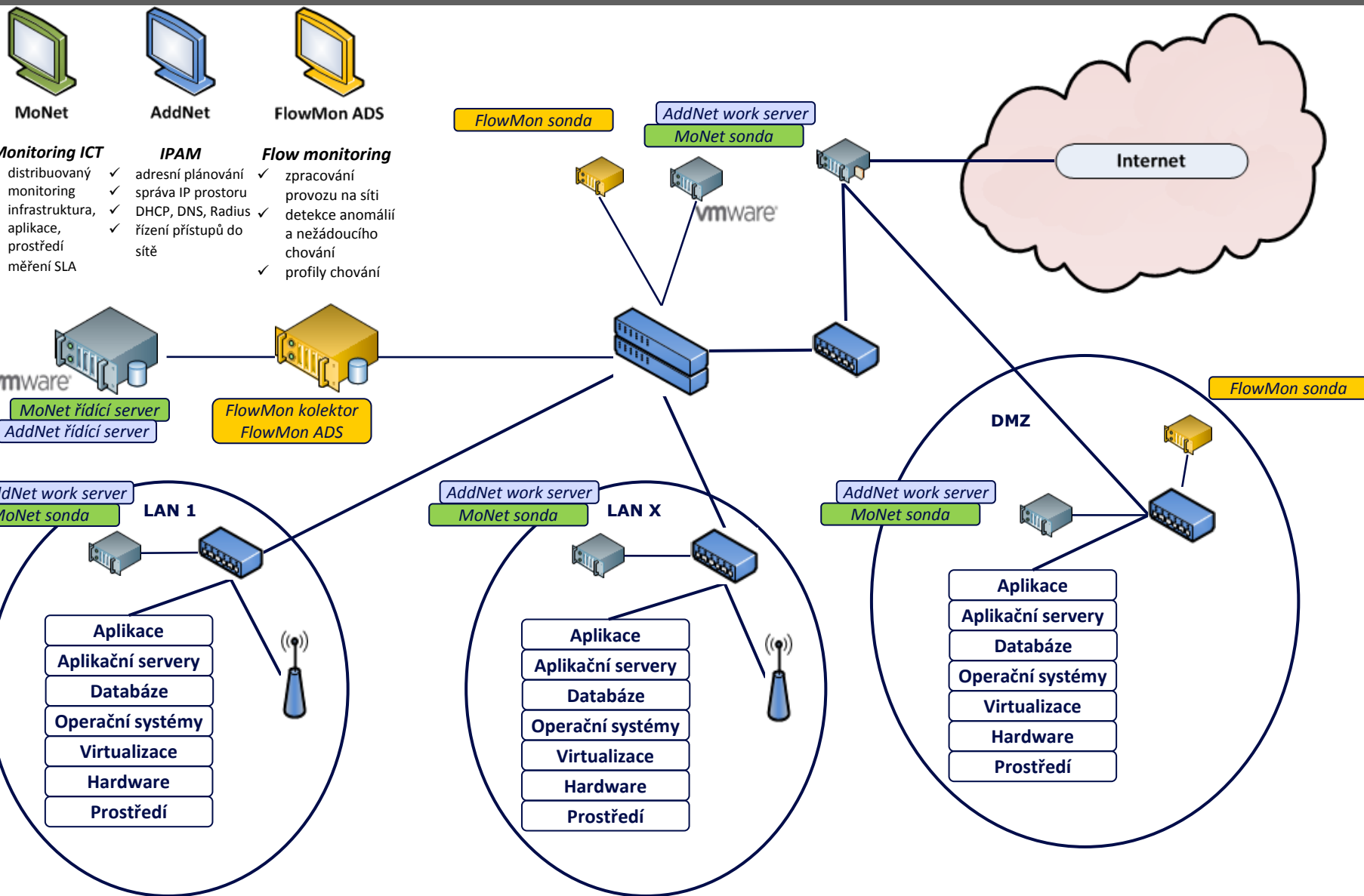


OP Vzdělávání
pro konkurenceschopnost

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

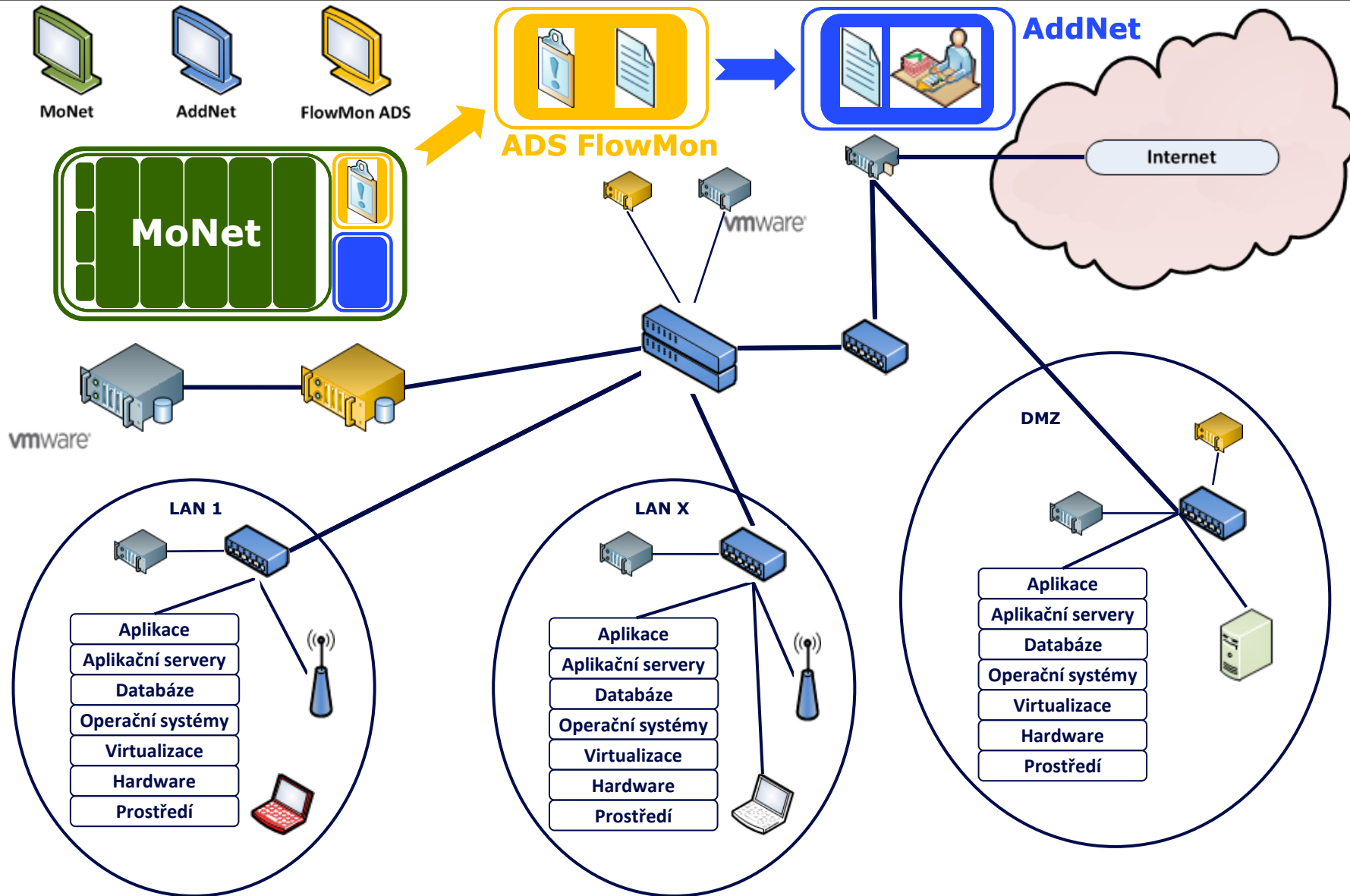


Centrální monitoring a správa sítě

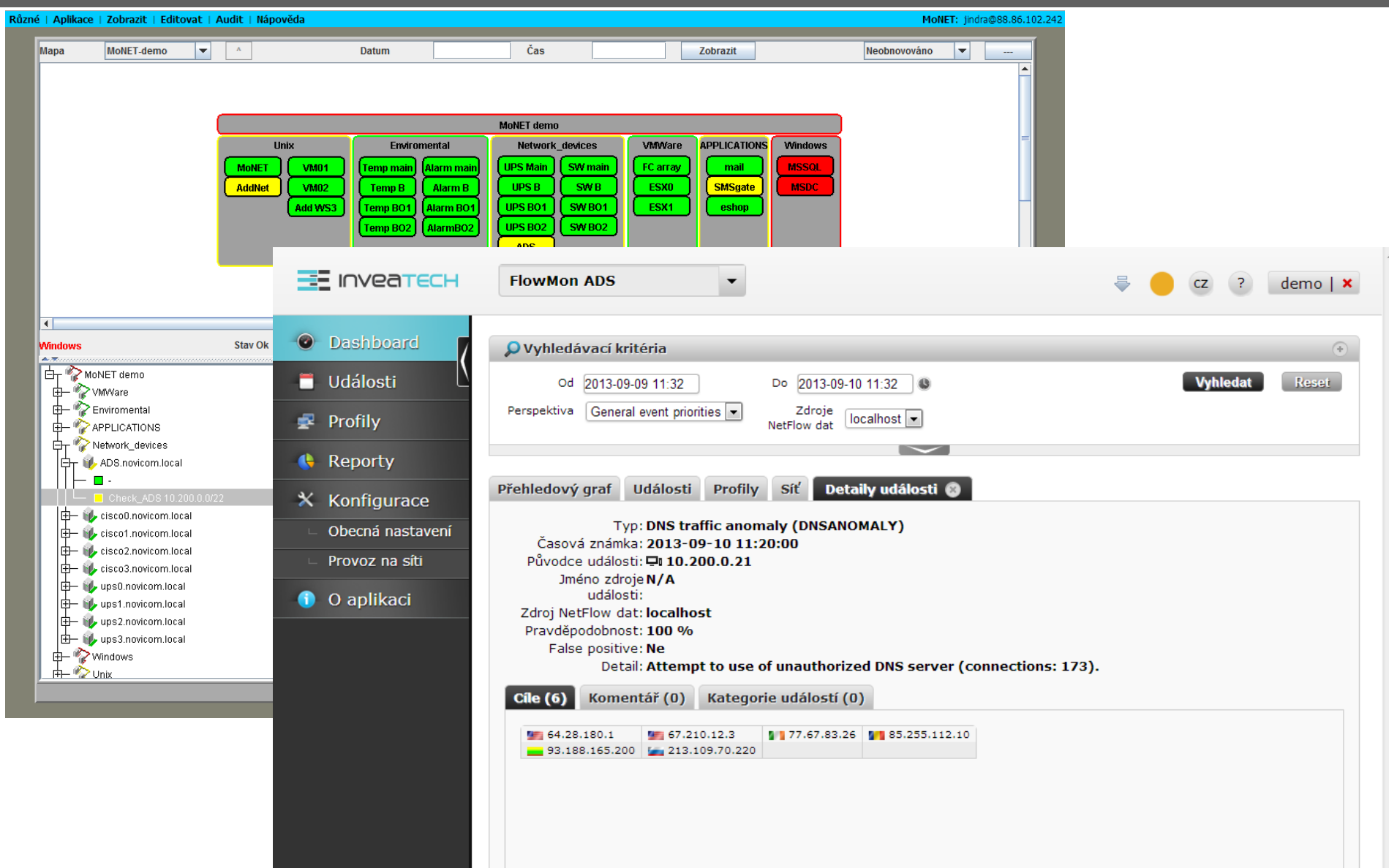


- **Základ pro spolehlivé a bezpečné fungování sítě**
- **Využití aktivních prvků s podporou 802.1x**
- **Při požadavku zařízení na síťovou komunikaci**
 - příslušný switch provede dotaz do integrovaného Radius serveru AddNetu, který dá informaci,
 - zda má zařízení povolenou komunikaci (802.1x & MAC autentizace)
 - případně zařadí zařízení do nastavené VLAN (autorizace)
- **Při požadavku na odpojení zařízení**
 - je tato informace opětovně distribuována přes Radius. Při opětovném dotazu (par. Positive time to live) je přístup odepřen a zařízení nemůže komunikovat na síti
- **Ověřeno s produkty**
 - Podpora heterogenních DDI a NAC řešení
 - Široké spektrum produktů
 - Switche, routery, wireless, multiservice access platformy a gatewaye,...





Koncept v detailu - MoNet => FlowMon ADS



The screenshot displays the FlowMon ADS interface. At the top, a navigation bar includes links for 'Různé', 'Applikace', 'Zobrazit', 'Editovat', 'Audit', and 'Nápověda'. The main window shows a 'MoNET demo' topology with various components like Unix, Environmental, Network_devices, VMWare, APPLICATIONS, and Windows. A sidebar on the left lists the network topology, including 'MoNET demo', 'VMWare', 'Environmental', 'APPLICATIONS', 'Network_devices', 'ADS.novicom.local', and 'Unix'. The main content area shows a 'Dashboard' with options for 'Události', 'Profily', 'Reporty', 'Konfigurace', 'Obecná nastavení', 'Provoz na síti', and 'O aplikaci'. The 'Události' (Events) section is active, displaying a search criteria form and a list of events. The event details for 'DNS traffic anomaly (DNSANOMALY)' are shown, including the time '2013-09-10 11:20:00', source IP '10.200.0.21', and a detail about unauthorized DNS server connections.

MoNET demo topology components:

- Unix: MoNET, AddNet, VM01, VM02, Add WS3
- Environmental: Temp main, Alarm main, Temp B, Alarm B, Temp BO1, Alarm BO1, Temp BO2, Alarm BO2
- Network_devices: UPS Main, SW main, UPS B, SW B, UPS BO1, SW BO1, UPS BO2, SW BO2
- VMWare: FC array, ESX0, ESX1
- APPLICATIONS: mail, SMSgate, eshop
- Windows: MSSQL, MSDC

Event Details:

- Typ: DNS traffic anomaly (DNSANOMALY)
- Časová známka: 2013-09-10 11:20:00
- Původce události: 10.200.0.21
- Jméno zdroje N/A
- události:
- Zdroj NetFlow dat: localhost
- Pravděpodobnost: 100 %
- False positive: Ne
- Detail: Attempt to use of unauthorized DNS server (connections: 173).

Related IP addresses:

64.28.180.1	67.210.12.3	77.67.83.26	85.255.112.10
93.188.165.200	213.109.70.220		



Vyhledávací kritéria

Od 2013-09-09 11:32

Do 2013-09-10 11:32

Perspektiva

General event priorities

Zdroje
NetFlow dat

localhost

Vyhledat

Reset

Přehledový graf

Události

Profily

Síť

Detaily události X

Typ: DNS traffic anomaly (DNSANOMALY)

Časová známka: 2013-09-10 11:20:00

Původce události: 10.200.0.21

Jméno

Různé Aplikace Topologie Volby Radius DNS Switche DHCP Adresní plánování Importy a exporty Přístup Protokol AddNet ARPMON_300 : [jindra edituje] jindra@10.200.0.10

Zdroj NetFlow

Pravděpodobnost

False

Cíle (6)

64.28.1

93.188

IP adresa: 10.200.0.21

MAC:

Hledat

Souhrnné informace

IP adresa 10.200.0.21
 MAC
 Výrobce NIC
 Přeložená IP (ads.novicom.local)
 IP adresa 10.200.0.21 spadá do sítě Office-10.200.0.0/24 (10.200.0.0/24)
 IP adresa 10.200.0.21 spadá do bloku Servers (10.200.0.16-10.200.0.63)

Pravidla

Typ	Povoleno	Krizový set	DHCP klient	IP adresy	
Statické nastavení	Y	Zakázat	Y	00:50:56:00:30:20 10.200.0.21	Smazat Upravit

IP

IP adresa	DNS	Síť	
10.200.0.21	ads.novicom.local	Office-10.200.0.0/24	Smazat Upravit

Díčí monitor

MAC	IP	Status	Přidělení	Jméno switche	Interface	Porty	Od	Do
00:50:56:00:30:20	10.200.0.21	Statický	Nepřřazeno		eth0		12.08.2013 18:24:34	10.09.2013 11:52:22
00:50:56:00:30:20	10.200.0.21	Statický	Nepřřazeno		eth0		12.08.2013 18:24:34	10.09.2013 11:51:33
00:50:56:00:30:20	10.200.0.21	Statický	Nepřřazeno		eth0		12.08.2013 18:24:07	10.09.2013 11:51:32
00:50:56:00:30:20	10.200.0.21	Statický	Nepřřazeno		eth0	10	28.06.2013 11:49:26	12.08.2013 17:37:22
00:50:56:00:30:20	10.200.0.21	Statický	Nepřřazeno		eth0	10	25.06.2013 10:12:28	12.08.2013 17:37:22
00:50:56:00:30:20	10.200.0.21	Statický	Nepřřazeno		eth0	10	17.06.2013 14:59:38	12.08.2013 17:37:22

Poslední stav dle IP

IP	MAC	Poslední DHCP	Poslední výskyt
10.200.0.21	00:50:56:00:30:20		10.09.2013 11:52:22

MoNet

AddNet

 FlowMon


Univerzální Monitoring

- Aplikace
- Aplikační servery
- Databáze
- Operační systémy
- Virtualizace
- Hardware
- Síťové prvky
- Prostředí

IPAM

- Správa IP adresního prostoru
- L2 Monitor – historie IP/MAC/locality

DDI – Základní síťové služby

- High Performance & distribuované DHCP
- Flexibilní & distribuované DNS

Bezpečnost

- 802.1x & MAC Autentizace
- Autorizace – VLAN přiřazení
- Distribuovaný RADIUS
- Krizové plánování

BYOD and mobilní zařízení

- Automatizovaná správa IP & NAC
- Samoobslužný management portal

Aktivní prvky

- Repository
- Port utilizace monitor
- Zálohování konfigurací

Sběr provozních dat

- NetFlow v5/v9/IPFIX
- L3/L4/I4 visibility
- Network performance monitoring
- On-demand packet capture

Provozní statistiky

- Objemové and provozní statistiky
- Drill down a datová analýza
- Vlastní profily a Reporting

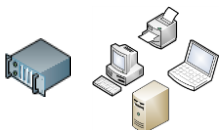
Behaviorální analýza

- Útoky, Malware, APTs
- Síťové anomálie, porušení politik
- Konfigurační a provozní problémy

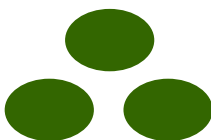
Dashboard

- Top and traffic statistics
- Bezpečnostní incidenty

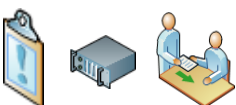
Nezávislý monitoring



Distribuovaný monitoring



Otevřený monitoring

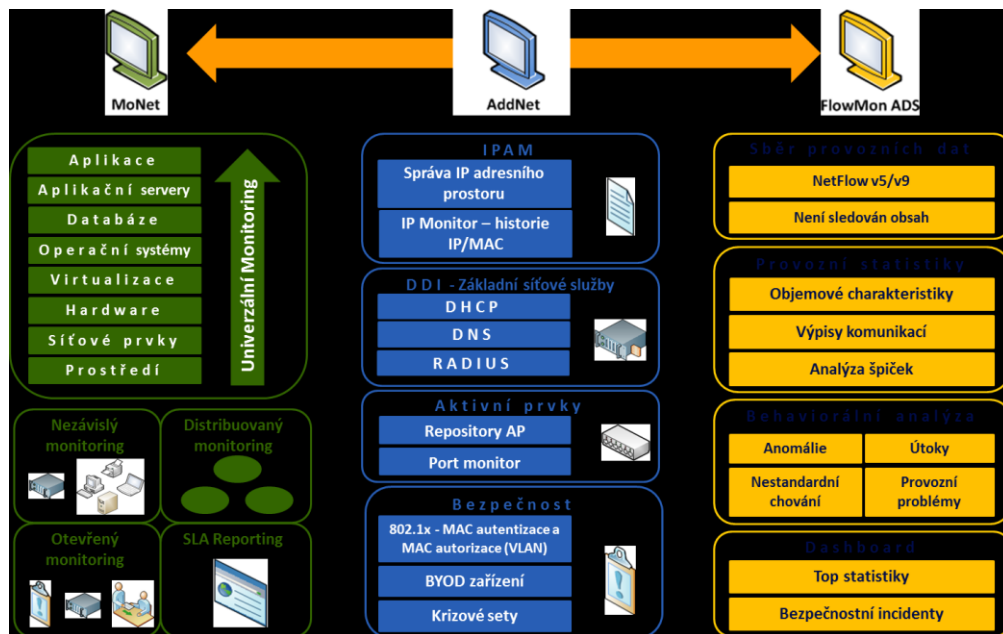


SLA Reporting



- **Ověření připravenosti k ZoKB**
- **Distribuovaný monitoring infrastruktury**
- **IPAM/DDI/L2 monitoring - distribuovaná správa IP adresního prostoru a základních síťových služeb (DNS, DHCP, RADIUS)**
- **NAC – distribuovaná 802.1x/MAC autentizace a autorizace**
- **Zálohování a podpora obnovy konfigurací aktivních prvků**
- **Ve spolupráci s INVEA-TECH**
 - Flow monitoring
 - NBA
 - Behaviorální analýza
 - APM

**Bezpečnost na
4 kliknutí**



■ Zajímavá služba pro stanovení dopadů ZoKB na organizaci



ZoKB assessment

Služby ověření úrovně kybernetické bezpečnosti

a porovnání s požadavky zákona 181/2014 Sb. - Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů

Výrazný nárůst používání informačních technologií v současném světě vede na jedné straně k vytvoření informační společnosti, urychlení komunikace a velkému rozvoji služeb a tím celé společnosti. Závislost společnosti a jejího fungování na informačních technologiích rapidně narůstá, a to ve všech oblastech (nejedná se pouze o služby informační společnosti jako je internetový obchod, ale i o fungování informačních systémů, na jejichž správné funkci je závislá celá řada základních služeb jako například řízení dopravy, přenos energií, výkon veřejné moci apod.). Se vzrůstající závislostí společnosti na informačních technologiích pak ale na straně druhé vzrůstá i riziko zneužívání těchto technologií nebo útoky na tyto technologie, které mají rozsáhlé dopady do činnosti subjektů, které s nimi pracují, a potencionálně mohou vést ke značným škodám.

V pátek 29. 8. 2014 byl ve Sbírce zákonů pod č. 181/2014 Sb. publikován zákon o kybernetické bezpečnosti. Přijetím této normy Česká republika reaguje na rizika zneužití informačních a komunikačních technologií s potenciálně značnými škodami.

Zákon odráží vzrůstající závislost společnosti na informačních technologiích, kdy riziko zneužití těchto technologií může mít rozsáhlé dopady a může vést ke značným škodám. Všechny vyspělé země, mezi něž Česká republika bezesporu patří, jsou již zcela závislé na správném fungování informačních a komunikačních systémů. Zákon bude účinný od 1. ledna 2015.

Protože problematika kybernetické bezpečnosti je s ohledem na okruh dotčených odborností značně rozsáhlá, připravili jsme pro vás službu, která vám usnadní orientaci v tom, jakým způsobem se tato věc týká právě vaší organizace a nakolik je vaše organizace připravena vypořádat se s povinnostmi, které jí touto normou budou uloženy.

Zkušení odborní konzultanti vám pomohou ve spolupráci s vámi provést

Ověření organizačních opatření (§ 5, odst. 1 zákona)

- Identifikace existujícího systému řízení bezpečnosti informací organizace
- Identifikace způsobu řízení rizik organizace
- Identifikace bezpečnostní politiky organizace a její aplikace
- Identifikace úrovně organizační bezpečnosti organizace a její aplikace

- **Novicom s.r.o.**
 - Koněvova 67
 - 130 00 Praha 3
 - www.novicom.cz
 - sales@novicom.cz

- **VUMS Datacom**
 - Šárka Business Park
 - Lužná 591
 - 160 00 Praha 6
 - www.datacom.cz
 -

- **Jindřich Šavel**
 - obchodní ředitel
 - jindrich.savel@novicom.cz
 - +420 271 777 231
 - +420 777 222 961

Novicom Channel Partner

