Kybernetická kriminalita jako významná bezpečnostní hrozba a možná řešení

Bc. Miroslav Černý
Sales Director

Praha, 1. 6. 2023

CYBER SECURITY & NETWORK MANAGEMENT
HAS NEVER BEEN EASIER

Kyberzločin roste a zisky jsou obrovské …

ČT24

Domů | Živé vysílání | Pořady ČT24 | Kauzy

Řecko na rozcestí | Uprchlická krize | Domácí | Regiony | **Ekonomika** | Svět | Kultura

Domů > Ekonomika

Kyberzločin - výnosnější byznys než drogy

13. 9. 2011 10:42, autor: duk
aktualizováno 13. 9. 2011 15:28

Velikost textu:

Praha – Každý den se stane obětí kyberzločinu více než jeden milion lidí. Vyplývá to ze studie Norton Cybercrime Report, kterou vydala společnost Symantec zabývající se zabezpečením počítačů. Celkové ztráty plynoucí z kyberzločinu a výdaje na řešení problémů s ním spojených podle studie ročně vystoupají na 114 miliard dolarů. Ztracený čas si oběti zločinů po síti cení na 274 miliard dolarů. Náklady spojené s počítačovou kriminalitou už dokonce převýšily objem světového trhu s drogami, jako je například heroin nebo kokain.

Kybernetické incidenty jsou teprve podruhé v historii průzkumu na prvním místě v barometru rizik Allianz, přerušení podnikání kleslo na těsné druhé místo a přírodní katastrofy jsou na třetím místě.
[zdroj: forbes.com 2022]

deník.cz

ZPRÁVY | PODNIKÁNÍ | SPORT | NÁZORY | MAGAZÍN | TIPY | MIMINKA | PRÁ

ČESKO | EVROPA PRO ČECHY | SVĚT | EKONOMIKA | REGIONY | KRIMI | KULTURA | ČEŠI V ČÍS

PŘEHLEDNĚ: Formulář pro opuštění okresu. Kde ho najdete, kam ho budete

Masivní ky
napadli ve

5.3.2021 | AKTUALIZOV

ČTK

Systém veřejn
kybernetické
(Piráti), data
i ministerstvo

Aktuálně.cz

Branou pro útoky na úřa
ruská firma sídlící v Čes

ČESKÝ ROZHLAS | RADIOŽURNÁL | PLUS | DVOJKA | VLTAVA | WAVE | ŽIVÉ VYSÍLÁNÍ | RE

22. BŘEZNA 2021 | LEONA | 5°C, OBLAČNO

iROZHLA

DOMOV | SVĚT | EKONOMIKA | SPORT | KULTURA | VĚDA | KOMENTÁŘE | ŽIVOTNÍ S

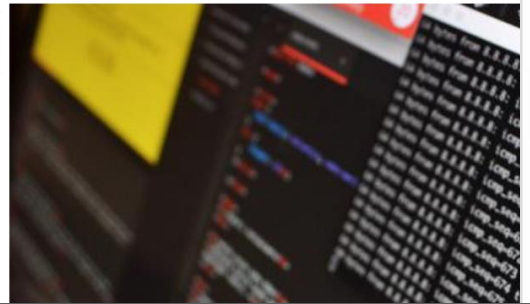
ONLINE: Koronavirus ve světě a v Česku – čtěte aktuální zprávy

Kde se nacházíte: iROZHLAS.cz / Zprávy z domova | Související témata: nemocnice hacker zdravotnické z
bezpečnost kybernetický útok koronavirus druhá vlna koronaviru koronavirus v Česku

Českou nemocnici opět napadli ha
jaké zařízení se jedná

Další českou nemocnici napadli hackeři. Podle kyberbezpečnost
využili vyděračský virus ransomware a zašifrovali některé syst
potvrdil i Národní úřad pro kybernetickou a informační bezpečn
nezveřejnily.

Praha 7:58 12. ledna 2021



LUPA.cz

Lupa.cz » Články »

Kybernetický útok vyjde draho, pre
vyplatí

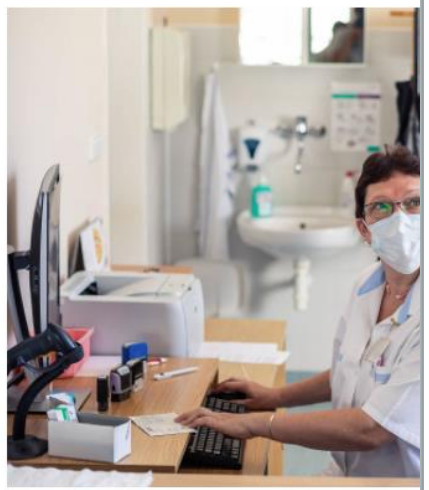
Aktuálně.cz

Sdílet článek | To se mi líbí

Kyberútoků na nemocnice je za dva měsíce skoro o polovinu víc, využívá se stavu nouze

HOSPODÁŘSKÉ NOVINY

Na ochranu před kyberútoky nemáme p
nepomáhá, tv
nemocnic. Ak
útočili



Fakultní nemocnici Brno vznikla při březnovém kyberr
Nemocnice přišla o některá administrativní a ekonom
autor: HN – Tomáš Škoda

Markéta Řeháková, redaktorka
16. 3. 2021 / 19:00 / 9 minut čtení

iDNES.cz / ZPRAVODAJSTVÍ

Domácí | Zahraničí | Krimi | Kraje | Ekonomika | Kultura | Finance | Revue

Škody po kyberútoku jsou obrovské, náprava potrvá měsíce, přiznal šéf ŘSD Mátl

23. května 2022 15:40

Ředitelství silnic a dálnic (ŘSD) se bude z kybernetického útoku minulého týdne vzpamatovávat měsíce, škody jsou obrovské, řekl šéf úřadu Radek Mátl. Útok narušil weby či účetnictví, stavby však neohrozil.

Ukrajina je i pod kybernetickým útokem | foto: Profimedia.cz

Podle Mátla šlo o propracovaný a dlouho připravovaný útok. Vedle webových stránek či asistenční linky nefungovaly po hackerském útoku například účetnictví, systém veřejných zakázek, spisová služba a další programy. Stavby ani řízení provozu by naopak ohroženy být neměly.

Praha bude v létě opět ztichlá, obává se šéf turistické centrály

Reklama

ÁRSKÉ NOVINY

li zdravotnické zařízení ministerstva
k se nezdařil, potvrdil Hamáček

deník.cz

PORT | NÁZORY | MAGAZÍN | TIPY | MIMINKA | PRÁCE | DO

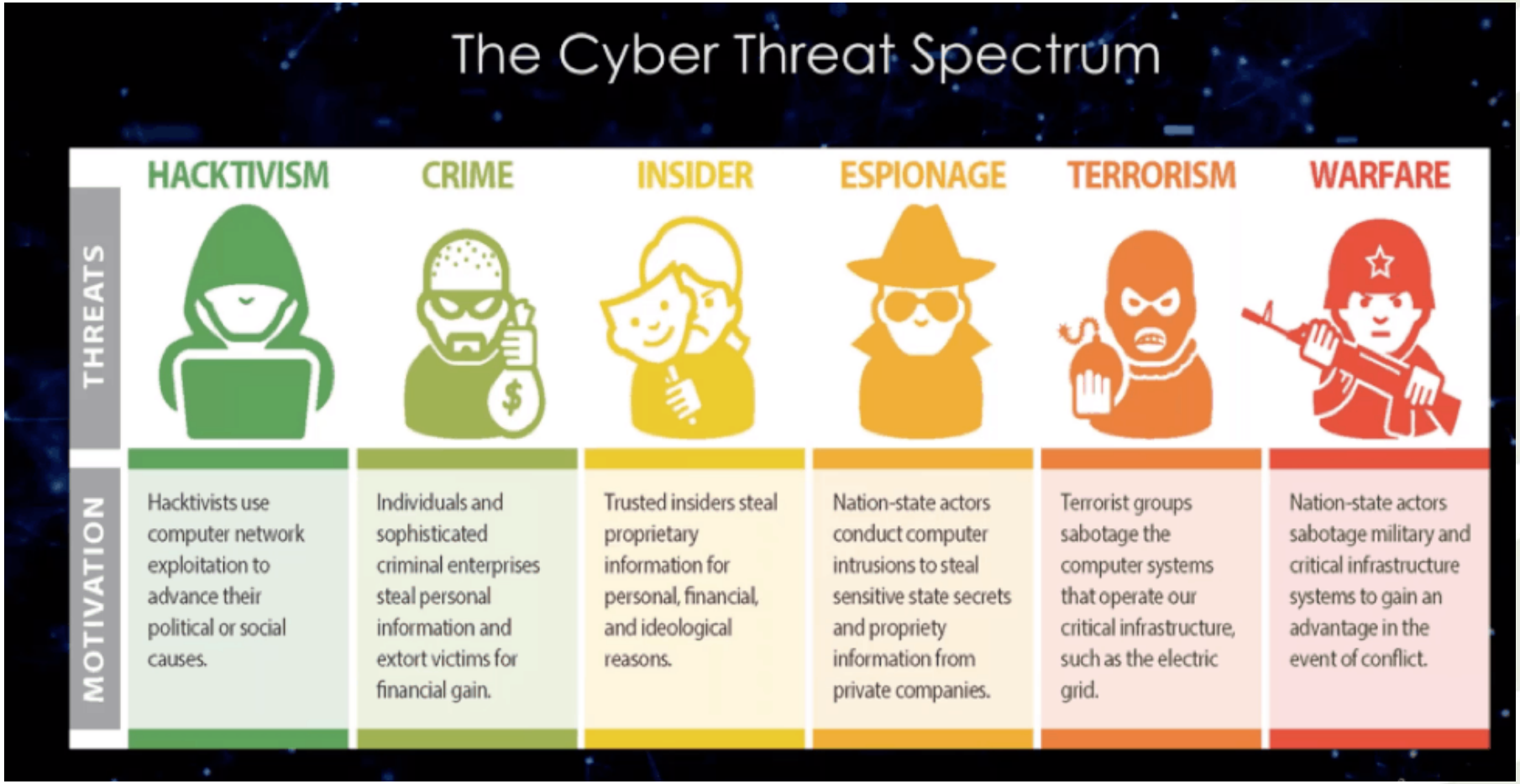
SVĚT | EKONOMIKA | REGIONY | KRIMI | KULTURA | ČEŠI V ČÍSLECH

pro opuštění okresu. Kde ho najdete, kam ho budete potřeb

erů. Napadli systémy Správy železnic,
e neohrozili

v minulých dnech napadli počítačové systémy Správy
organizace však nijak provoz ani bezpečnost na
padem se nyní zabývá Národní úřad pro
mační bezpečnost (NÚKIB). Upozornil na to dnes
ili na sítě státních organizací i v minulých týdnech.

Typy kybernetických útočníků …



[Zdroj: technically Technical]

Kyberzločin jako služba CaaS (Crime as a service)

Dark Web Hackers — Products | Register | Login

Welcome to the Dark Web Hackers

Have you tried to buy hacking services on the dark web before? Not happy with the results? Only empty promises but no one getting the job done?

Then you should try Vladimir and George, the dark webs most trusted hackers for getting things done.

Unlike others, our prices are not the cheapest, but if we can't do a job, you will get a full refund!

Vladimir

Hello, my name is Vladimir.
I am the technical expert at dark web hackers.

My expertise is programming, running exploits, setting up DDOS attacks and i like the challenge of doing things where most others give up.
I can "recover" passwords of most social networks easily, remote control smartphones, and most other things that are useful because i spent years to find methods that really work.
Here you can find a list of my services, if it is not listed, then minimum price will be $600 and we will discuss the final price once you gave me all information and i accept the job.

[zdroj: darkweb]

Product	Price	Quantity
Remote control the phone of someone else, most new models supported	700 USD = 0.01737 ฿	1 X Buy now
Facebook and Twitter account hacking	500 USD = 0.01241 ฿	1 X Buy now
Other social network account hacks, for example reddit or instagram	450 USD = 0.01117 ฿	1 X Buy now
Full package deal, getting access to personal or company devices and accounts and searching for the data you need.	1800 USD = 0.04466 ฿	1 X Buy now
DDOS for protected websites for 1 month	900 USD = 0.02233 ฿	1 X Buy now
DDOS for unprotected websites for 1 month	400 USD = 0.00992 ฿	1 X Buy now
Hacking webservers, game servers or other internet infrastructure	1300 USD = 0.03226 ฿	1 X Buy now
30 days full service, i will work 8 hours per day for 30 days only on your project	9500 USD = 0.23571 ฿	1 X Buy now
Other services, final price will be discussed	600 USD = 0.01489 ฿	1 X Buy now
Only additionaly: Add this item if your target is a high profile VIP or large public company	2500 USD = 0.06203 ฿	1 X Buy now
Only additionally: priority service or 1 full day extra work for complicated cases	400 USD = 0.00992 ฿	1 X Buy now

Kyberzločin v kyberprostoru…

2022 CRIME TYPES, *Continued*

INTERNET CRIME COMPLAINT CENTER

VICTIM OVER 60 LOSSES

Crime Type	Loss	Crime Type	Loss
Investment	$990,235,119	Spoofing	$22,261,276
Tech Support	$587,831,698	SIM Swap	$19,515,629
BEC*	$477,342,728	Data Breach	$17,681,749
(Reporting a potential business loss)	*$369,773,371*	Extortion	$15,555,047
(Reporting a personal loss)	*$107,569,357*	Phishing	$14,453,929
Confidence/Romance	$419,768,142	Overpayment	$10,977,231
Government Impersonation	$136,500,338	Employment	$6,403,021
Real Estate	$135,239,020	Malware	$1,851,421
Personal Data Breach	$127,736,607	Threats of Violence	$376,458
Lottery/Sweepstakes/Inheritance	$69,845,106	Harassment/Stalking	$254,659
Credit Card/Check Fraud	$61,649,198	Ransomware**	$210,052
Non-payment/Non-Delivery	$51,531,615	IPR/Copyright and Counterfeit	$203,140
Advanced Fee	$49,322,099	Botnet	$120,621
Identity Theft	$42,653,578	Crimes Against Children	$48,373
Other	$31,410,237		

[Zdroj: FBI IC3]

Počet zařízení (notebooků a stolních počítačů), tabletů a mobilních telefonů používaných na celém světě bude podle společnosti Gartner, Inc. v roce 2021 činil celkem 6,2 miliardy kusů.

Došlo k významným průlomům, jako jsou Solar Winds, Colonial Pipeline a desítky dalších …

Ransomware přišel s pomstou zaměřenou na mnoho malých a středních podniků.

Snad nejznepokojivější bylo, jak byla slabá místa zabezpečení kritické infrastruktury a dodavatelských řetězců cílena a zneužívána protivníky ve vyšší míře než v minulosti.

[zdroj: forbes, autor Chuck BROOKS]

Kybernetická bezpečnost

Management

Bezpečnostní management a přístup aktivního dohledu SOC

Procesy

Analýzy stavu a rizik, hodnocení aktiv, řízení rizik, ISMS, ISO 27001:2022

Lidé

Vzdělávání zaměstnanců a pravidelný trénink, evaluace

Technologie

Integrovaná správa sítě a podpora v rozsáhlých sítích IPAM, DHCP, DNS, NAC, L2 …

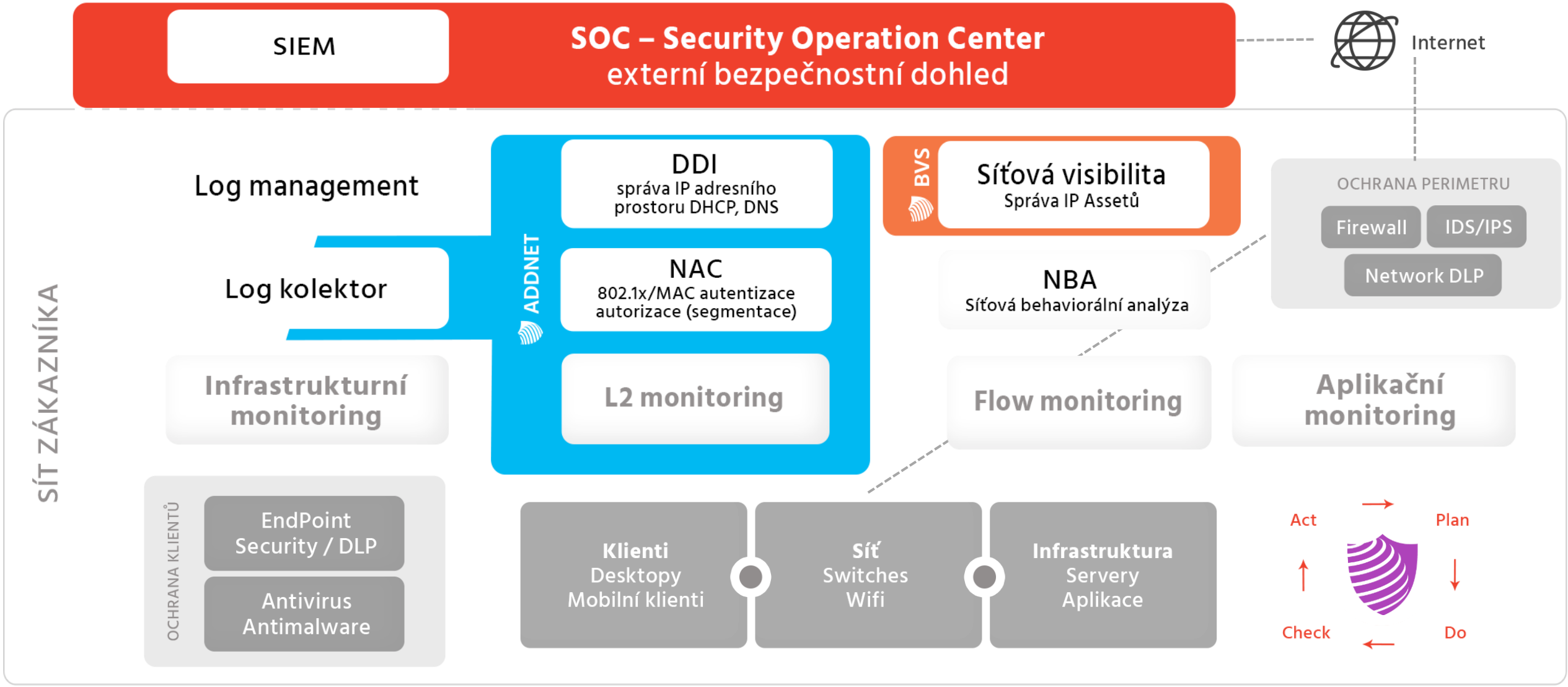
Novicom

- **Český výrobce řešení pro efektivní správu, monitoring a zabezpečení sítí**

- **Orientujeme se na:**
  - střední a velké zákazníky
  - zákazníky vyžadující vysokou míru bezpečnosti a provozní spolehlivosti svých sítí

- **Na IT trhu prosazujeme přístup aktivního bezpečnostního dohledu (SOC)**

Naplnění bezpečnostní vize Novicomu



Pohled Novicomu na oblast kybernetické bezpečnosti

Závažný globální problém

- **Nárůst počtu i závažnosti kybernetických incidentů**
- **Známé útoky v ČR**
  - Nemocnice Benešov, FN Ostrava, FN Brno, OKD, ŘSD…
  - *Škody jsou ve výši stovek miliónů Kč*
  - *Neschopnost provozovat svůj business*

Proč se to děje?

- **Podcenění managementem organizací**
  - není chápána závažnost problematiky
  - není ochota věnovat tomu adekvátní zdroje (finanční a lidské)
- **Kybernetická bezpečnost je svěřována přímo IT oddělení**
  - IT je zaměřeno na zajištění provozu a za to je i hodnoceno
  - kybernetická bezpečnost odčerpává IT lidské zdroje a finance pro zajištění jejich primárního cíle

Více otázek než odpovědí…

Vyřeší to nákup technologií pro kybernetickou ochranu?

Ano, ale:

- **Jsou zapotřebí pro desítky oblastí**

Monitoring, detekce, řízení technologií, ochrana koncových bodů…

- **Opravdu je k dispozici kvalifikovaná obsluha?**

Která je připravena a je si jistá, co dělat v případě útoku?

- **Opravdu máte tuto kvalifikovanou obsluhu nepřetržitě k dispozici?**

Režim 24 x 7 x 365

- **Opravdu se vám to vyplatí?**

Vybudování týmu se znalostmi, které umožňují postavit se v reálném čase hackerům, je pro více než 90 % organizací ekonomicky nereálné!

Řešení problému

- **Řešením je sdílení specializovaných zdrojů kybernetické ochrany se specialisty:**
  - **SOC – Security Operation Center** – služba vrcholového bezpečnostního dohledu
- **Bezpečnostní monitoring nabízí kde kdo. Jaký je ten správný?**
  - Pouze SOC **připravený plně převzít zodpovědnost za boj s hackery a být schopen provádět obranné reakce kdykoliv**, bez součinnosti s administrátory zákazníka
- **Vize aktivního SOCu**
  - Aktivní SOC může nabídnout bezpečnost 24x7 a proaktivní incident response pouze v případě, **že se zákazníkem sdílí nástroje zajišťující vhled do sítě a řízení sítě**
- **Vizí Novicomu je poskytovat sofistikované technologie a know-how, které zákazníkům usnadní jejich připojení k aktivnímu SOCu**

Novicom řešení pro vizi aktivního SOCu

- **Organizační a metodická příprava zákazníků**
  - Řízení systému kybernetické bezpečnosti
  - Vzdělávání v oblasti kybernetické bezpečnosti
- **Integrovaná správa sítě**
  - Sdílené využívání integrovaného nástroje pro
    - L2 monitoring – lokalizace zařízení v síti
    - DDI (IPAM/DHCP/DNS) – správu IP adresního prostoru a síťových služeb
    - NAC – řízení přístupu do sítě, včetně segmentace a mikrosegmentace
- **Podpora správy a monitoringu v rozsáhlých sítích**
  - Distribuovaný model řízení sítě DDI/NAC a monitoring vzdálených lokalit
    - L2, netflow/IPfix, syslog
- **Úplná visibilita aktiv a jejich komunikace**
  - Vizualizace a klasifikace IT aktiv a jejich komunikace
- **Podpora rozhodování při řešení incidentů**
  - Vyšetřování komunikace aktiv a znalost důsledků nedostupnosti aktiv na provozované business služby (aplikace)

CONSULTING

ADDNET

BVS

ADDNET

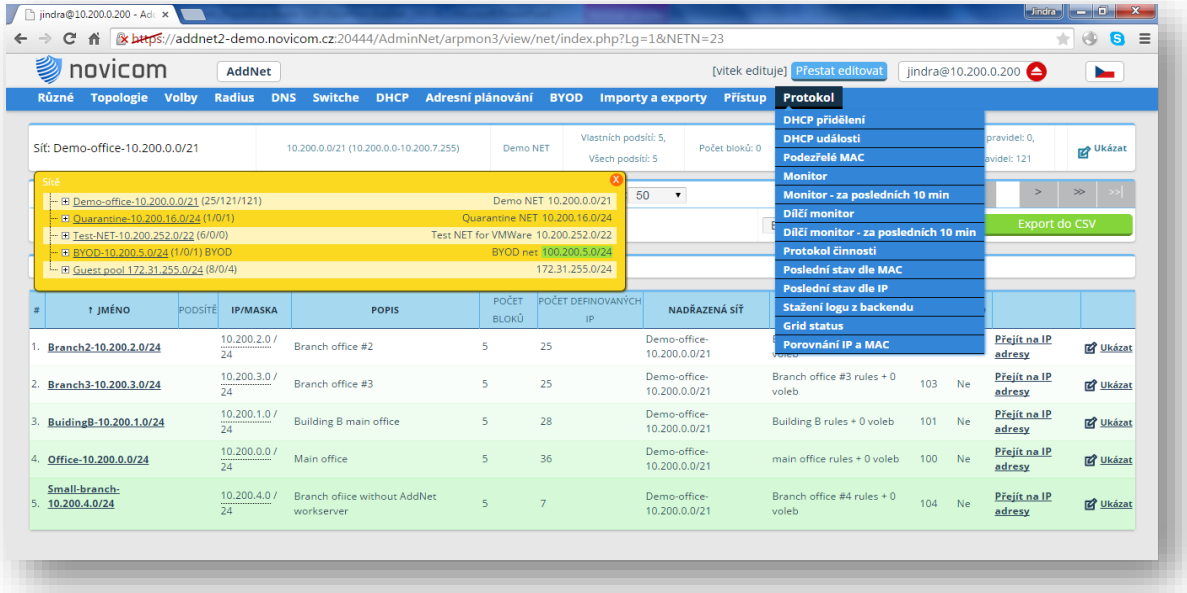
Novicom ADDNET

Unikátní **Multivendor** DDI/NAC nástroj přinášející zásadní zjednodušení a zvýšení efektivity správy IP adresního prostoru a řízení bezpečnosti přístupu v rozsáhlých sítích.

Novicom ADDNET

Je unikátní **DDI/NAC nástroj** pro zajištění **řádového zvýšení efektivity správy IP adresního prostoru a řízení bezpečnosti přístupu v rozsáhlých sítích**.

Toho je dosaženo **integrací systémů** L2 monitoringu, správy IP adresního prostoru, základních síťových služeb (DHCP, DNS), řízení přístupu do sítě (NAC), pokročilé komunikace s aktivními prvky sítě.

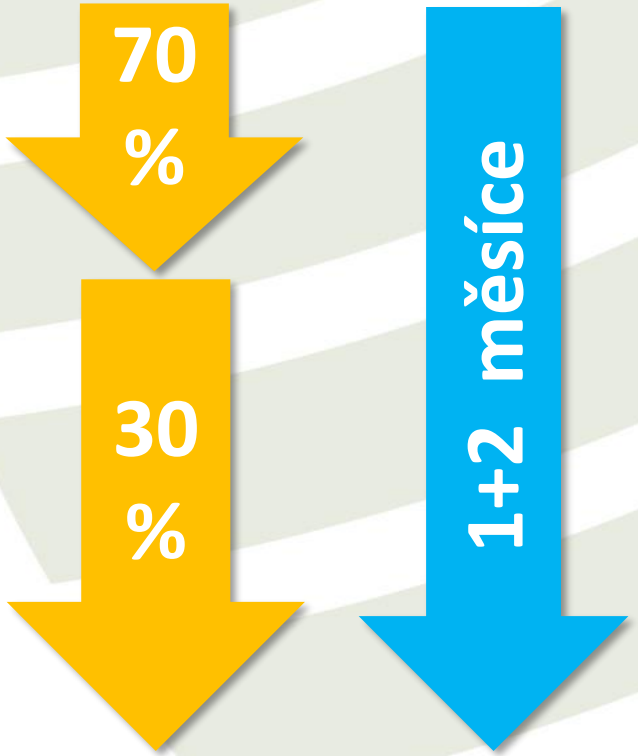


ADDNET – klíčové přínosy

- √ **L2 monitoring** - lokalizace zařízení v síti a úplná historie stavu sítě
- √ **Řádové snížení pracnosti síťové správy**
- √ **Standardizace činností a centralizace správy** v rozsáhlých sítích
- √ **DDI – zavedení integrovaných základních síťových služeb (IPAM/DHCP/DNS)**
- √ **NAC – snadné zavedení a správa**
  - Autentizace - full 802.1x a/nebo MAC
  - Autorizace - řízení VLAN/mikrosegmentace
- √ **Pokročilé síťové politiky**
  - Prevence nákaz typu ransomware
  - Automatizovaná správa důvěryhodných zařízení – trusted pools
- √ **BYOD – automatizovaná správa a identifikace BYOD a mobilních zařízení**
- √ **Zvýšení provozní spolehlivosti DDI/NAC služeb** díky vícenásobné redundanci a nadstandardní škálovatelnosti
- √ **Úspora nákladů** díky sledování utilizace aktivních prvků, zvýšené produktivitě apod.
- √ **Plná heterogennost -** bezproblémová spolupráce běžnými síťovými technologiemi
- √ **Schopnost okamžité reakce** na kybernetické bezpečnostní incidenty
- √ **Podpora konceptu Aktivní SOC**
- √ **Snadná implementace** a ověřené projektové postupy – NIM metodika

Snadné nasazení ADDNETU

- Využití původní Novicom implementační metodiky NIM
- Grid Manager – efektivní systémový setup
- Hlavní fáze
  - Vstupní analýza
  - Příprava SGP infrastruktury
  - Aplikační nastavení ADDNETU
  - Iniciační sniffing (L2)
  - Nastavení finální IP strategie
  - Spuštění vizualizace a správy IT aktiv
  - Spuštění DDI / NAC
  - Nastavení integrací (MS AD, NBA, SIEM…)
  - Zahájení provozní podpory



NIM
Novicom Implementation Methodology

Další informace o Novicomu?

Sledujte nás na:

- www.novicom.cz
- LinkedIn
- Facebook
- YouTube

Kontaktujte nás na:

- E-mail: sales@novicom.cz
- Tel.: +420 271 777 231

Nebo osobně:

- Miroslav ČERNÝ, Sales Director
- E-mail: miroslav.cerny@novicom.cz
- Mobil: +420 603 251 159

Adresa:

- Novostrašnická 176/39, 100 00 Praha 10

SUDOP GROUP

novicom

CYBER SECURITY & NETWORK MANAGEMENT
HAS NEVER BEEN EASIER


ADDNET

BVS

CCM

ACADEMY

APPLIANCE