


Postaráme se o maximální ochranu vašich citlivých dat. V naší nabídce najdete programy, které ochrání váš hardware i software jak před únikem informací, tak před narušením či přesměrováním služeb.



Viry, červi a jiný nežádoucí software číhá dnes na každém rohu. Chraňte svá citlivá data a zabezpečte svůj počítač včas. K trhlinám v bezpečnosti systému dochází navzdory ochranným opatřením jeho tvůrců. Infikovat počítač nežádoucím softwarem je snadné, stačí podcenit pravidelnou aktualizaci.

**Jsme experti na** antivirovou ochranu, firewally, bezpečnostní a penetrační testy, logování přístupů, analýzu, EMS, Azure RMS i Data Loss Prevention.

## NEJVĚTŠÍ HROZBY UPLYNULÉHO ROKU

Hackeři jsou vynalézavější než kdy dříve. Jejich útoky se odhalují nejhůře v tzv. aplikacích „na míru“. Nechceme vás strašit, ale data mluví za vše. Jen ve zkratce:

- útoky invazivního kódu Backdoor a vyděračských programů Ransomware vzrostly o více než 40 %
- s internetovým útokem se už setkalo 30 % všech počítačových uživatelů
- antiviry zachytily přes 21 mil. unikátních škodlivých objektů
- hackeři cílí stále častěji i na cloud
- škodlivé kódy, které těží kryptoměny, sílí
- a na vzestupu jsou i dříve ojedinělé multiplatformové útoky

## CO BUDE DÁL?

Extrémně rychlé mobilní sítě ještě více usnadní útoky hackerů z pohledu rychlosti a kapacity. V bezpečí nebudou počítače, chytré telefony ani routery. Útočníkům půjde hlavně o sabotáž chodu firem a veřejné infrastruktury. Umělá inteligence bude více koketovat s temnou stranou síly. Zintenzivní útoky na IoT a dojde k únikům stovek milionů hesel a údajů o uživateli, které budou zneužívány pro krádeže identit a phishingové útoky.

Blíží se konec klasických, za pár vteřin nabouratelných, hesel. O slovo se bude stále více hlásit dvoufaktorové ověřování, biometrické metody i kryptograficky založené hardwarové klíče.

To, co zní jako hodně dobrý thriller, je bohužel realitou. Jste si stále jistí, že máte vše pod kontrolou?

# IT bezpečnost

nwt®  
efektivní ICT

Mobile  
device

## BEZPEČNOSTNÍ A PENETRAČNÍ TESTY

Obstojí váš podnikový software před útokem hackerů? Ověřte si, zda je opravdu neprůstředný a odhalte, kde se skrývají vaše největší slabiny. Nabízíme profesionální penetrační testy webových aplikací, e-shopů, serverů i lokálních sítí a další služby pro bezpečný chod vaší společnosti.

## LOGOVÁNÍ A MONITORING

Máte přehled o tom, co se děje ve vašem síťovém prostředí? Říká se, že co oči nevidí, srdce nebolí - v případě IT bezpečnosti to ale rozhodně neplatí. Hackerský **útok vás může naprosto ochromit.**

Dokážeme detekovat i hrozby, proti kterým jsou ostatní bezpečnostní nástroje neúčinné. Přinášíme kompletní řešení pro monitorování a bezpečnost počítačových sítí (nejen) na základě IP toků. Využíváme inteligentní shromažďování logů a informací ze sítě a jejich následné zpracování, vyhodnocení a poskytnutí relevantních informací o aktuálním stavu.

Mezi naše přední nástroje patří např. FlowMon a Gigamon.

## ANALÝZA IT BEZPEČNOSTI

**Ochráníme vaše důvěrná data** a posvítime si i na takové hrozby, jako je zneužití zranitelnosti HW i SW, získání dat zaslaných nezabezpečenými komunikačními kanály nebo jejich zkopírování pro třetí strany, ať už pomocí hardwarových zařízení nebo sociálního inženýrství.

## SOFTWAREVÝ AUDIT

Zjistíte, jestli je váš podnikový hardware a software skutečně legální, anebo se tak jen tváří. Nic to neproověří lépe než audit. Porovnáme instalované licence s těmi zakoupenými a upozorníme vás na potencionální hrozby v porušování autorského zákona. **Diskrétnost nadevše.** Výsledky auditu jsou výhradně interní záležitostí a slouží pouze pro účely společnosti.

## Microsoft Enterprise Mobility + Security (EMS)

Napadení nemusí být na první pohled viditelné. Přestože hackeři využívají stále agresivnějších nástrojů, jejich **útoky jsou mnohem sofistikovanější** a více cílené než kdy dříve.

**EMS** – se postará o veškerý komfort a bezpečí při využívání oblíbených aplikací a zařízení. Umožní vám:

- řízení identity a přístupu v cloudu
- ochranu identity
- správu mobilních zařízení a aplikací
- ochranu informací

## AZURE RMS

Ochranná služba založená na cloudu zabezpečí vaše soubory a e-maily díky sofistikovanému šifrování identit a zásad autorizace. Funguje napříč všemi zařízeními – telefony, tablety i počítači. Informace je možné chránit jak v rámci organizace, tak mimo ni.

## DATA LOSS PREVENTION

S DLP softwarem budete mít citlivá firemní data vždy pod kontrolou. Data jsou chráněna jak v klidu (uložena na disku), tak „v pohybu“ (na přenosných médiích).

Za pomoci šifrování a kryptování zabrání DLP únikům dat z jednotlivých pracovních stanic společnosti, zajistí jejich ochranu proti odcizení a postará se také o to, aby k privátním informacím měli přístup pouze legitimní uživatelé.