

## Bezpečnosť v kocke

Nedovoľte prístup k Vaším dôverným informáciám.

Ohrozuje stabilitu Vašej organizácie únik informácií?  
Zverujú Vám zákazníci citlivé dáta?

Únikom informácií sú ohrozené predovšetkým personálne dáta, obchodné informácie a know-how. Útočníci prenikajú k cenným informáciám zvnútra i zvonku, zachytávajú tiež dáta prenášané po súkromných i verejných sieťach.

Naše produkty a služby overia úroveň ochrany Vašich informácií a potom pre ne vytvoria bezpečné prostredie.

### ZMAPOVANIE STAVU

#### Penetračné testy

Overíme úroveň ochrany Vašich dát pred zneužitím. Pokúsime sa pomocou najmodernejších metód prieniku zachytiť a prečítať prenášané dáta a preniknúť zvnútra i zvonku k uloženým citlivým informáciám. Úspešné prieniky analyzujeme a navrhujeme nápravné opatrenia, ktoré im účinne zabránia.

#### Informačný audit

Analyzujeme technický a bezpečnostný stav IT infraštruktúry v organizácii. Posúdime stav Vašich telekomunikačných služieb, vrátane nákladov. Na základe získaných výsledkov navrhujeme optimálne nápravné opatrenia. Zvyšujeme výkon, znižujeme náklady, zlepšujeme business.

### STABILIZÁCIA STAVU

#### Ochrana komunikačnej infraštruktúry siete

Zabezpečujeme Vašu sieťovú infraštruktúru pred možnými útokmi

### VYLADENÉ KOMUNIKÁCIE

zvonku i zvnútra. Vašu sieť chránime pred nežiadúcim sledovaním. Projektujeme a komplexne vystavujeme chránené miesta, v ktorých sú umiestnené dátové centrá a ostatné dôležité komponenty infraštruktúry IT.

#### Ochrana serverov a staníc

Znemožňujeme nežiadúci únik obsahu uložených správ, kódovaním chránime emaily, súbory a databázy. Vytvárame optimálnu a účinnú koncepciu antivírovej a antispýwarovej ochrany organizácie. Implementujeme prostriedky ochrany vrátane dodávky vhodného hardware a software.

Poskytujeme OUTSOURCING KOMPLEXNEJ ANTIVÍROVEJ OCHRANY.

### NASTAVENIE AKTÍVNEJ BEZPEČNOSTI

#### Integrácia monitoringu, reporting

Mapujeme pokusy útočníkov získať alebo poškodiť Vaše uložené a prenášané informácie. Identifikujeme ciele útokov a pomôžeme odhaliť i pôvodcu a zdroj útokov. Integrujeme roztrieštené monitorovacie nástroje do jedného

účinného. Zjednodušujeme obsluhu, znižujeme náklady, zvyšujeme efektívnosť. Neoddeliteľnou súčasťou je systém reportingu podľa Vašich potrieb a požiadaviek.

### Implementácia prvkov aktívnej bezpečnosti

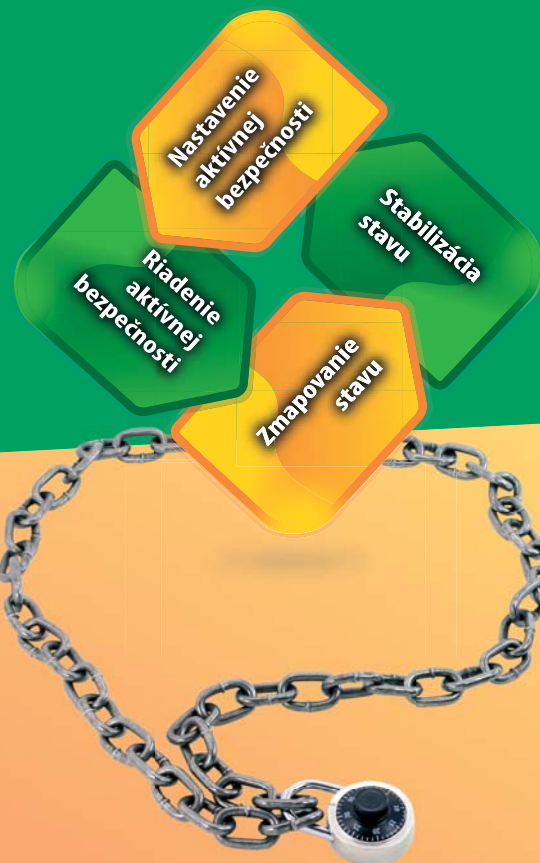
Vytvoríme Vaše IT prostredie tak, aby bolo aktívne proti útočníkom. Nasadením nástrojov proaktívnej bezpečnosti umožníme automatickú reakciu bezpečnostných prvkov skôr, než dôjde k bezpečnostnému incidentu.

### RIADENIE AKTÍVNEJ BEZPEČNOSTI Formalizácia

Zjednotíme celú Vašu dokumentáciu týkajúcu sa bezpečnosti IS/IT. Uskutočníme optimalizáciu dokumentácie a zakomponujeme ju do súčasných procesov organizácie.

### Systém riadenia bezpečnosti (ISO)








Prečo vymýšľať už raz vymyslené a overené? Prečo zvyšovať náklady na chod organizácie? Zavedieme systém riadenia bezpečnosti informácií podľa medzinárodných pravidiel a štandardov. Zaisťujeme Vám bezpečné a preverené dáta.









# Štruktúra produktov

## Riziká a ich ošetrovanie.

### PENETRAČNÉ TESTY







-  Možný únik informácií
-  Znemožnenie podnikania
-  Finančné straty
-  Overenie úrovne ochrany dát
-  Zvýšenie bezpečnosti informačných systémov
-  Doporučené metódy ochrany
-  Efektívnejšie plánovanie investícií v oblasti IT

### INFORMAČNÝ AUDIT







-  Vysoké náklady
-  Nedostupné kritické aplikácie organizácie
-  Kompromitácia prostredia IS/IT
-  Zistenie stavu infraštruktúry organizácie
-  Optimalizácia hlasových a dátových služieb
-  Preverenie stavu bezpečnosti IS/IT









### OCHRANA KOMUNIKAČNEJ INFRAŠTRUKTÚRY SIETE

-  Nechránená komunikácia
-  Riziko odposluchu
-  Zahľtenie informačných systémov organizácie
-  Bezpečná komunikácia s partnermi
-  Dohľad, servis, bezpečnosť
-  Minimalizácia straty dát







### OCHRANA SERVEROV A STANÍC

-  Útoky vedúce k úniku informácií
-  Zničenie databázy dát
-  Strata obchodného tajomstva
-  Dáta bez škodlivého software
-  Zvýšenie celkovej bezpečnosti organizácie
-  Zabezpečenie integrity a dôvernosti







### INTEGRÁCIA MONITORINGU, REPORTING

-  Únik citlivých informácií
-  Zložité zisťovanie odkiaľ a kto útočí
-  Extrémne vysoké náklady na ochranu
-  Ochrana systému pred útočníkmi
-  Zistenie zdroja nebezpečenstva
-  Zistenie bezpečnosti systému







### IMPLEMENTÁCIA PRVKOV AKTÍVNEJ BEZPEČNOSTI

-  Neskoré zistenie útočníka
-  Finančné straty
-  Znemožnenie podnikania
-  Proaktívne reakcie na útok
-  Maximálna ochrana dát
-  Zachovanie know-how

### FORMALIZÁCIA

-  Roztrieštenosť a neprehľadnosť dokumentácie
-  Neznalosť obsahu dokumentácie
-  Nevymáhateľnosť dodržiavania predpisov
-  Zjednotenie dokumentácie
-  Jednoduchá správa noriem, predpisov a vyhlášok v organizácii
-  Ucelený systém

### SYSTÉM RIADENIA BEZPEČNOSTI

-  Zníženie konkurencieschopnosti
-  Zložité vnútorné procesy
-  Absencia bezpečnostnej politiky
-  Súlad s medzinárodnými štandardmi
-  Vysoká miera efektivity
-  Minimalizácia rizík IS