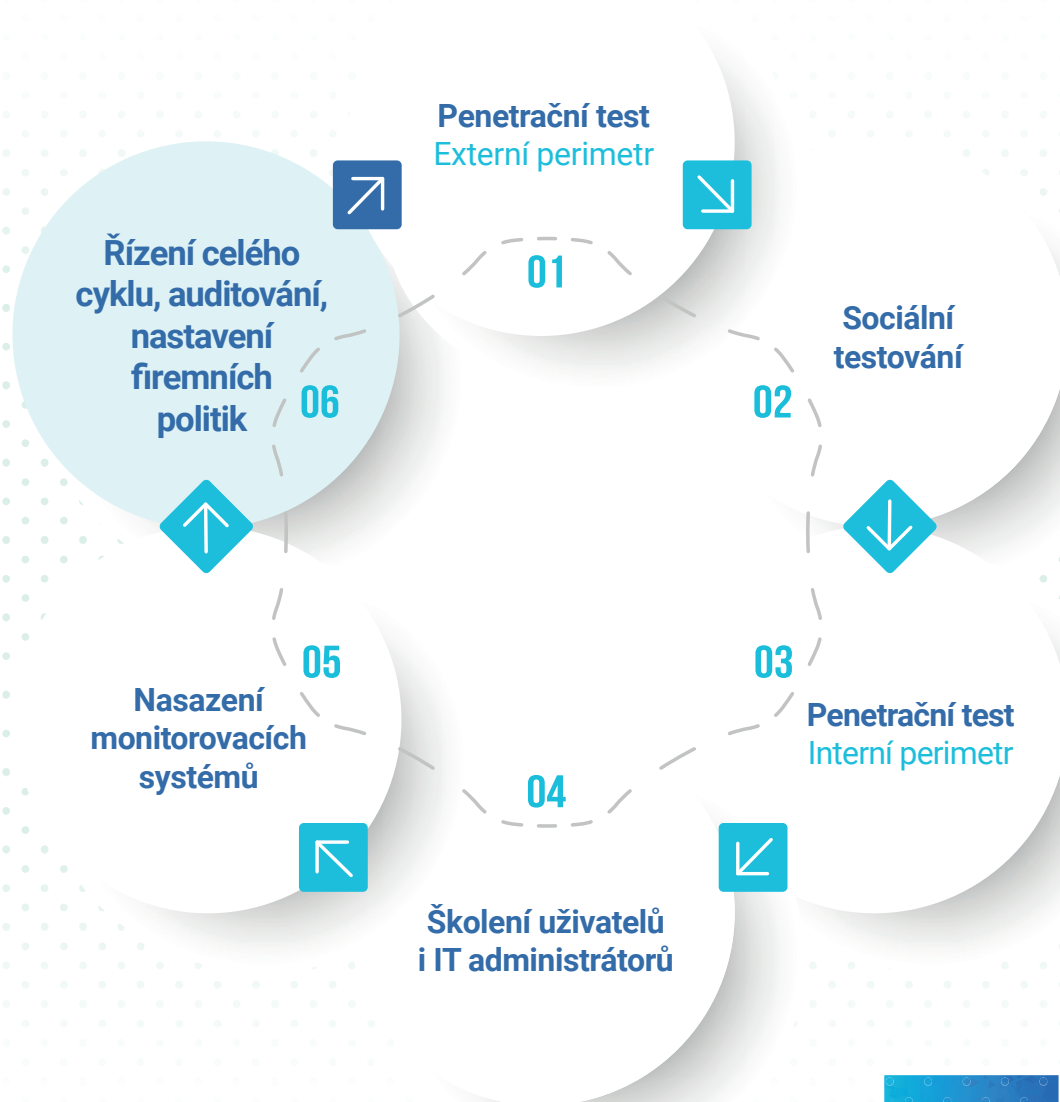


Ucelené pojetí služeb kybernetické bezpečnosti na míru klienta ✓

Kybernetická bezpečnost se často spojuje s termíny jako **analýza rizik, řízení zranitelností, audit ISO / IEC 27000 a dalšími**. Je zde množství konceptů kybernetické bezpečnosti a diskuze, jak je správně aplikovat. My v Direct IT věříme, že je dobré prověřovat bezpečnost hlavně prakticky a aplikovat přesně taková opatření, která vyžaduje situace klienta.

Míra komplexity zabezpečení a dané potřeby jsou totiž vždy poněkud odlišné.

Postupujeme krok za krokem a pro každého klienta definujeme ty nejdůležitější služby a opatření, tak abychom **dosáhli maximálního zabezpečení sítě a dat a zvedli jej o desítky procent z aktuálního stavu**.



Neváhejte nás kontaktovat pro více informací a ukázkou platformy
www.directit.cz | info@direct.cz | +420 775 466 513

DIRECTiT
applications

DIRECTiT
cybersecurity

DIRECTiT
consulting



Penetrační testování → Externí perimetr

- ▶ Prověříme Váš externí perimetr způsoby, jako by Vás chtěl napadnout skutečný hacker.
- ▶ Provedeme analýzu veřejných zdrojů a najdeme vše, co se o Vaší společnosti dá zjistit.
- ▶ Detailním skenem internetu se pokusíme dohledat i uniklé přihlašovací údaje.



Sociální testování

- ▶ Pokud dobře zabezpečíte externí perimetr, další cestou do vnitřní sítě mohou být lidé.
- ▶ Testujeme gramotnost Vašich zaměstnanců a zjistíme, jak by odolali například podvodným emailům při tzv. phishingovém útoku.



Penetrační testování → Interní perimetr

- ▶ Pokud by se útočník dostal do sítě přes uživatele, je důležité mít dobře zabezpečenou i vnitřní síť. Často tomu tak bohužel nebývá.
- ▶ Při testování sítě z interního perimetru se snažíme ovládnout celou doménu a poté i zálohy. Takto by postupovali i skuteční hackeři. My vás však nezašifrujeme, ale vyhotovíme komplexní zprávu o stavu Vaší bezpečnosti.



Školení uživatelů i IT administrátorů

- ▶ Školíme jak běžné uživatele, tak hlavně i IT administrátory, kteří musí často bezpečnost nastavovat.
- ▶ Pro školení lze kombinovat e-learning, multimediální platformy i fyzické on-site školení.



Nasazení monitorovacích systémů

- ▶ Pomůžeme Vám s nasazením monitorovacích systémů, abyste byli schopni útoky detekovat.



Řízení celého cyklu, auditování, nastavení firemních politik a další

- ▶ Bez papírů to nepůjde.
- ▶ Aby celá bezpečnost fungovala jako udržitelný koncept, musí být ve společnosti nastaveny určité politiky, které se musí dodržovat.
- ▶ V případě hackerského útoku Vám například disaster recovery plán ušetří nemalé množství času.



Vzhledem k neustálému rozvoji technologií, je potřeba celý cyklus a jeho části pravidelně opakovat a renovovat. Díky našemu portfoliu disponujeme těmi nejlepšími odborníky v oboru, které Vám můžeme pro jednotlivé fáze cyklu poskytnout.

eCPPTv2 | CEH | OSCP | CCNA | EITCA/IS | CISSP | CHFI | CompTIA PenTest+
Toto jsou certifikace, kterými disponují naši bezpečnostní konzultanti.

Neváhejte nás kontaktovat pro více informací a ukázkou platformy

www.directit.cz | info@direct.cz | +420 775 466 513