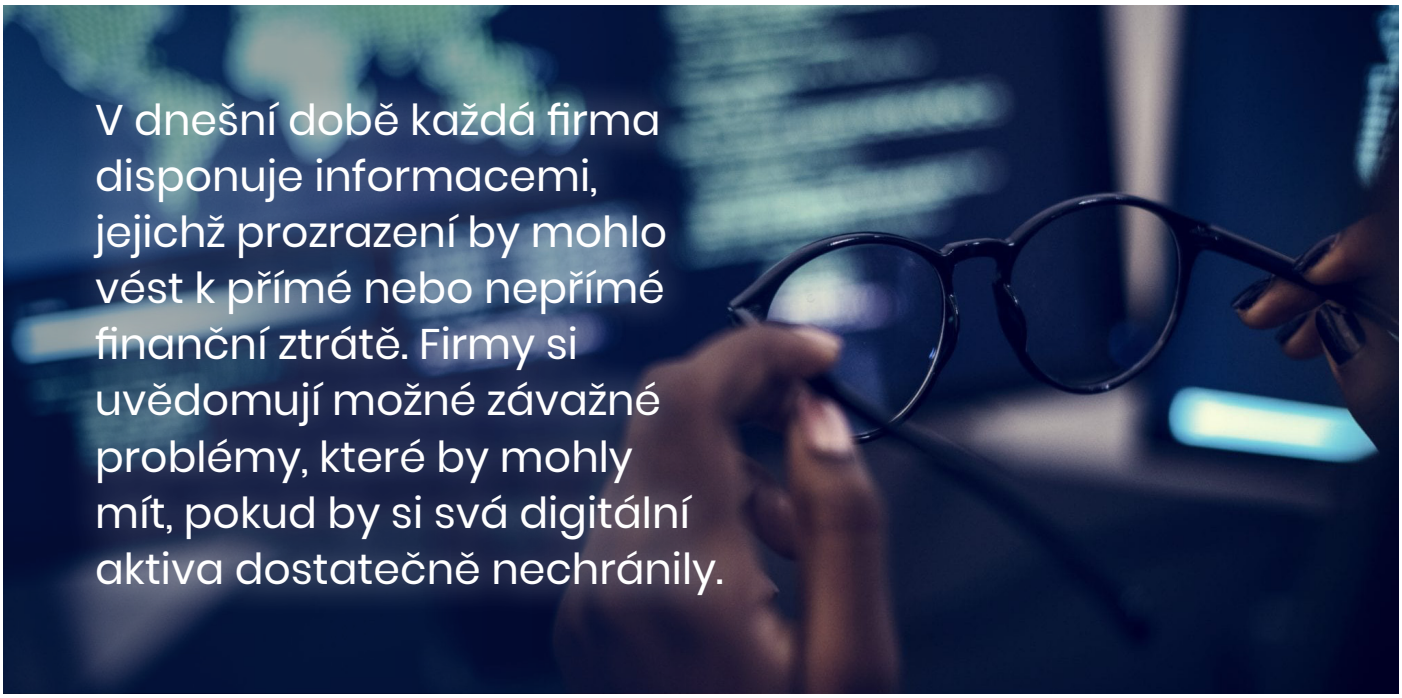
IT analýza



Prozrazení důvěrných dat mohou způsobit různé formy útoků. Hrozby, jako zneužití zranitelností firemních webových aplikací, získání dat zaslaných nezabezpečenými komunikačními kanály nebo zkopírování dat pro třetí strany pomocí hardwarových zařízení, jsou jen některé z důvodů, proč by IT administrátoři měli využívat bezpečnostní produkty jako řešení pro enkrypci, antivirus, DLP nebo firewally pro různé úrovně modelu OSI. Konfigurace těchto prvků vyžaduje čas a lidské zdroje.

Analýza otvírá oči vedení organizace o reálném stavu jejich IT a o tom jak IT pomáhá dosáhnout obchodních cílů organizace. Analýza bezpečnostních rizik je součástí kontinuálního procesu ochrany informací.

Analýza vychází z naší vlastní metodiky. Při zpracování nabídky bereme v úvahu individuální požadavky na analýzu, organizační strukturu a možnosti vlastního IT. Nabídku vždy přizpůsobujeme konkrétní organizaci.

Jak probíhá náš bezpečnostní audit

Krátká řízená interview s určenými pracovníky

Kontrola vybraných pracovišť

Kontrola dokumentace

Zpracování výsledků

Závěrečný workshop s prezentací výsledků

Ing. Filip Lang | filip.lang@ictnwt.cz | +420 724 707 417

ictnwt.cz

IT analýza

Neřeší vaše firma pravidelné bezpečnostní audity? Může to mít velmi vážné důsledky.

Naše řešení je adaptivní, rychlé a nenáročné

- Přizpůsobení konkrétním podmínkám organizace/ úřadu;
- rychlé získání výsledků;
- minimální nároky na zainteresované pracovníky;
- přehledné grafické vyjádření výsledků;
- doporučení k odstranění nedostatků.

Analýzy IT je možno zpracovat ve dvou variantách:

- popisná – zdokumentování aktuálního stavu používaných IT;
- bezpečnostní – zhodnocení a popis úrovně bezpečnosti používaných IT.

Příklad útoku v praxi

V Německu pravděpodobně zemřela žena kvůli ransomwaru. Napadená byla nemocnice v Düsseldorfu, kvůli čemuž bylo nutné pacienty převážet jinam. Ženu bylo nutné dopravit do nemocnice ve Wuppertalu, což znamenalo 32 kilometrů jízdy navíc. Útočníci využili nezáplatovanou zranitelnost ve VPN softwaru od Citrixu, přičemž záplata byla k dispozici od ledna. Proti útočníkům bylo zahájeno stíhání. Více na bleepingcomputer.com

Příklad útoku v praxi

V Benešovské nemocnici zablokoval kryptovirus fungování počítačů, paralyzoval počítačovou síť a lékaře připravil o jejich přístroje. Provoz nemocnice musel být výrazně omezen. Několik pacientů, kteří v nemocnici leželi a potřebovali podporu techniky, se muselo přestěhovat do jiných nemocnic a sanitky vozily nové pacienty rovnou jinam.
Zdroj: www.ct24.cz

Analýzu zaměřujeme na:

- fyzickou a logickou strukturu IT;
- používaný HW a SW;
- strukturovanou kabeláž;
- konektivitu k síti Internet;
- telefonní, popř. jiný používaný komunikační systém;
- rozsah, druh a charakter zpracovávaných dat;
- systém napájení IT;
- systém zálohování a archivace dat;
- systém obnovy SW a HW (zajištění kontinuity činností);
- systém fyzické bezpečnosti IT;
- systém personální a administrativní bezpečnosti IT.

Naše služby využívají

Parabel s.r.o. SOLUTIONS FOR YOUR VISIONS

R. JELÍNEK Original Czech Distilleries

SPUR

DF PARTNER

Ing. Filip Lang | filip.lang@ictnwt.cz | +420 724 707 417 ictnwt.cz