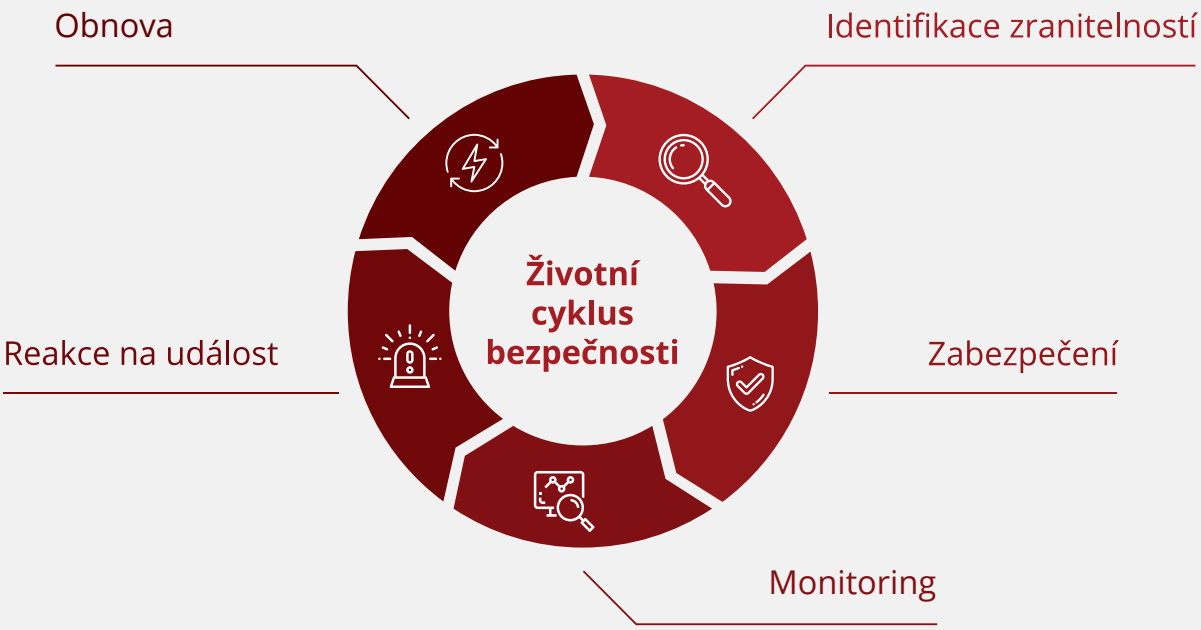
XEVOS | IT Solutions

# CYBER SECURITY

Ochrana zdrojů, dat a služeb.

# Služby kybernetické bezpečnosti

Kybernetickou bezpečnost považujeme za jednu z **klíčových hodnot** každé organizace. Skutečně funkční a komplexní řešení je dle našeho pohledu spíše **procesem** nežli cílovým stavem a zahrnuje opatření nejen technická, ale také organizační a personální. Pozornost je tak potřeba věnovat kromě **konfigurace** a **monitoringu** mj. také **vzdělávání uživatelů**. Naši odborníci disponují mnohaletými zkušenostmi z oblasti firemního i individuálního zabezpečení jednotlivých zařízení, komunikace i celkové infrastruktury a mohou vám tak být nápomocni ve všech fázích tohoto procesu.




- **Zhodnocení** aktuálního stavu a identifikace zranitelných míst *(analýza rizik, penetrační testy, atd.).*
- **Návrh** a **implementace** účinných a dostupných opatření *(antivirový systém, firewall, atd.).*
- **Školení** a **testování** uživatelů.
- **Řešení** bezpečnostních incidentů.
- Naplnění normativních, vnitrofiremních, nebo **legislativních požadavků** *(např. GDPR).*

XEVOS | Cyber Security

## KONZULTAČNÍ SLUŽBY

- Analýza současného stavu
- Analýza rizik
- Bezpečnostní dokumentace
- Fyzická bezpečnost
- Reakce na bezpečnostní incident

## IMPLEMENTACE ŘEŠENÍ

- Antivirová ochrana
- Business Critical Support 24/7
- Infrastruktura a architektura sítě
- Monitoring a proaktivní ochrana
- Ochrana dat únikem
- Ochrana dat před ztrátou (DLP, DRP)
- Zabezpečení elektronické pošty
- Správa mobilních zařízení (MDM)
- Webový filtr

## TESTOVÁNÍ

- Penetrační testy
- Zátěžové a (D)DoS testy
- Sociální inženýrství

## LEGISLATIVA A NORMY

- Ochrana osobních údajů (GDPR)
- Normy řady ISO/IEC 27000
- Zákon o kybernetické bezpečnosti

## ŠKOLENÍ

# KONZULTAČNÍ SLUŽBY

## Analýza současného stavu

- rámcový **náhled na zabezpečení** vybrané části systému *(např. architektura sítě, ochrana proti malware, správa uživatelů a rolí, fyzická bezpečnost)*
- výchozí dokument k většině konzultačních a implementačních činností

## Analýza rizik

- komplexní a hloubková analýza **současného stavu**.
- identifikace veškerých HW, SW a informačních *(zpravidla nejhodnotnějších!)* **aktiv**, výčet jejich **zranitelností,** možných **hrozeb**, a odhad pravděpodobnosti, že dojde k jejich naplnění a návrh účinných a dostupných řešení k jejich eliminaci
- **klíčový dokument** pro procesy řízení bezpečnosti a řízení rizik

## Bezpečnostní dokumentace

- bezpečnostní dokumentace pro procesy řízení bezpečnosti a řízení rizik *(např. bezpečnostní politika, příručka uživatele či správce, plán zálohování a obnovy)*
- dokumenty vychází ze závěrů **analytických** činností, výsledků **testů** a **auditů**, či interních plánů a strategií
- závazné dokumenty, dle kterých jsou udržovány procesy řízení bezpečnosti a řízení rizik v souladu s definovanými potřebami a cíli

## Fyzická bezpečnost

- zhodnocení zabezpečení HW aktiv před fyzickým **poškozením**, či **odcizením**.
- mezi rizikové faktory patří např. **nevhodná teplota** *(systém chlazení, klimatizace, protipožární systém)*, **neoprávněný přístup** *(přístupový a kamerový systém)*, **kontakt s vodou** apod.
- návrh vhodných **opatření k eliminaci** těchto rizik

## Reakce na bezpečnostní incident

- **forenzní analýza** dostupných informací *(např. logy, kamerové záznamy apod.)*
- návrh a realizace bezpečnostních opatření vedoucích k **zabezpečení** systému, **nápravě** škod *(např. obnova ze záloh)*, či **odhalení** pachatele.

# IMPLEMENTACE ŘEŠENÍ

## Antivirová ochrana

- ochrana systému před viry a dalším škodlivým SW
- návrh optimálního řešení, instalace, vzdálená správa a komplexní servis

## Business Critical Support 24/7

- **neustálá (24/7)** odborná technická **podpora**
- vyřešení požadavku do dalšího pracovního dne

## Infrastruktura a architektura sítě

- restrukturalizace a rekonfigurace logické či fyzické sítě v souladu s **bezpečnostními požadavky** *(např. oddělení interní a externí sítě, DMZ)*
- instalace a konfigurace **nových** bezpečnostních prvků *(např. firewall, IPS/IDS)*
- **rozšíření** sítě dle aktuálních potřeb *(optimalizace datových toků, zvýšení výkonu, bezdrátové pokrytí, atd.)*
- správa cloudových řešení *(např. Cisco Meraki).*

## Monitoring a proaktivní ochrana

- optimalizace logovacích aktivit systému *(např. priorita dostupnosti nebo důvěrnosti).*
- řešení zálohy logů
- **predikce problémů** dříve, než k nim skutečně dojde *(upozornění na chybějící bezpečnostní aktualizaci, upozornění na nečitelné sektory na HDD, atd.)*

## Ochrana dat před únikem

- **zabezpečení před únikem citlivých údajů** *(přihlašovacích údajů, osobních údajů, firemního know-how, obchodního tajemství, apod.)*
- Ochrana všech částí systému *(HW, SW, komunikace, procesy, politiky)*

## Ochrana dat před ztrátou (DLP, DRP)

- implementace a správa široké škály řešení poskytujících **zálohu** a **obnovu dat** pro koncové stanice, síťovou komunikaci i servery
- specializace na **cloudová řešení**
- klasifikace dat i vypracování plánu zálohy a obnovy *(DRP)*

## Ochrana elektronické pošty

- opatření chránící vaši emailovou schránku před nevyžádanou poštou *(SPAM).*

## Správa mobilních zařízení (MDM)

- systém pro jednotnou a přehlednou správu a zabezpečení **veškerých** mobilních zařízení v organizaci *(soukromé a firemní mobilní telefony, tablety)*
- podpora široké škály zařízení a všech rozšířených operačních systémů *(iOS, Android, Windows Phone, BlackBerry)*

## Webový filtr

- **centralizovaná kontrola** nad přístupem uživatelů sítě k webovým stránkám
- databáze založená na manuální klasifikaci
- široká škála využití *(např. zamezení prokrastinace zaměstnanců, ochrana dětí před nevhodným obsahem, ochrana proti phishingu a ransomware)*

# TESTOVÁNÍ

## Penetrační testy

- prověření bezpečnostních mechanismů z pohledu externího útočníka *(hackera)*
- testování probíhá **simulací útoku na síťovou infrastrukturu**, její část *(Wi-Fi síť),* nebo konkrétní aplikaci *(webovou či mobilní).*
- výstupem je přehledná závěrečná zpráva s návrhem vhodných protiopatření

## Zátěžové a (D)DoS testy

- testování systému na několik druhů útoků typu (D)DoS, jejichž cílem je znepřístupnit systém
- závěrečná zpráva s grafickým znázorněním reakce systému včetně návrhu vhodných protiopatření

## Sociální inženýrství

- prověření dosavadních praktik uživatelů vašeho systému metodami sociálního inženýrství *(např. email a voice phishing)*
- cílem je **zjištění pravděpodobnosti**, že by mohlo tímto způsobem dojít k úniku **citlivých** informací
- výstupem je závěrečná zpráva a školení uživatelů.

# LEGISLATIVA A NORMY

## Ochrana osobních údajů (GDPR)

- soulad s požadavky **General Data Protection Regulation (GDPR),** resp. nařízení EU č. 2016/679 o ochraně osobních údajů fyzických osob, *(např. zaměstnanců, zákazníků, či dodavatelů).*
- analýza současného stavu nakládání s osob. údaji,
- návrh a implementace opatření
- ustanovení role pověřence pro ochranu osobních údajů *(Data Protection Officer)*

## Normy řady ISO/IEC 27000

- audit systému a řízení bezpečnosti informací *(ISMS)* **v souladu s normami** řady ISO/IEC 27000.
- podrobná analýza současného stavu
- návrh a **implementace opatření**
- vypracování dokumentace, **měření** a **hodnocení** účinnosti implementovaných opatření

## Zákon o kybernetické bezpečnosti

- analýza a řízení procesu **souladu činnosti systému** s požadavky Zákona o kybernetické bezpečnosti *(č. 181/2014 Sb.),* který se vztahuje na vybrané subjekty provozující tzv. **základní služby**[1]
- analýza současného stavu plnění povinností
- návrh a **implementace opatření**
- vypracování dokumentace

# ŠKOLENÍ

> „ **Uživatele lze vždy považovat za nejslabší článek každého ICT systému!** “

- proškolení uživatelů vašeho systému v bezpečném nakládání s informacemi
- snaha o minimalizaci pravděpodobnosti **úniku citlivých informací** chybou uživatele
- před školením je možno prověřit dosavadní praktiky uživatelů metodami sociálního inženýrství

[1] *Služba, jejíž poskytování je závislé na sítích nebo IS a jejíž narušení by mohlo mít významný dopad na zabezpečení klíčových společenských nebo ekonomických činností v některém z těchto odvětví: energetika, doprava, bankovnictví, infrastruktura finančních trhů, zdravotnictví, dodávky a rozvody pitné vody, digitální infrastruktura, chemický průmysl a veřejná správa.*

Společnost XEVOS Solutions poskytuje komplexní IT řešení – od systémové integrace, servisu a podpory, přes cloudová, serverová, síťová a tisková řešení, až po dodávky HW a SW vybavení.

Našim cílem je pomáhat organizacím i jednotlivcům zvyšovat efektivitu a chránit jejich činnosti a podnikání. V posledních letech se velmi úzce specializujeme na oblast kybernetické bezpečnosti a s tím související ochranu našich zákazníků.

Mezi primární aktivity společnosti patří především IT podpora a servis HW i SW řešení, kde se profilujeme jako nezávislý servisní partner. Tyto služby poskytujeme jak na našich pobočkách tak především on-site přímo u našich zákazníků. V oblasti servisu veškerých PC zařízení, periferií a komponent jsme vytvořili servisní centrum, ve kterém zajišťujeme opravy všech běžně dostupných značek na trhu.

Provádíme záruční i pozáruční opravy. Nabízíme serverová, cloudová i klientská řešení pro firmy a domácnosti při využití platforem PC i MacOS, tiskových řešení, prezentační techniky, tabletů i chytrých telefonů.

Veškeré implementace a odborné práce realizované společností XEVOS provádějí odborně vyškolení specialisté, kteří úspěšně absolvovali náročné zkoušky, testy a jsou držiteli prestižních certifikátů světových firem. Tyto certifikáty, společně s velkými praktickými zkušenostmi, dokazují naši vysokou odbornost a kvalitu.

## REFERENCE

Orava

MYSTIC PRODUCTION

HOBES

Bivoj

## CERTIFIKACE

Certifikační společnost VUPS ISO 9001 Výzkumný ústav pozemních staveb

Zelená firma®

Certified Associate
Mac Integration 10.12

XEVOS | IT Solutions

+420 591 140 315
ostrava@xevos.eu

XEVOS Solutions s.r.o.,
28. října 1584/281, 709 00 Ostrava

www.xevos.eu