sofogroup®

... solutions for organisations

SOFO BEZPEČNÁ KOMUNIKACE

Pro koho je program SOFO Bezpečná komunikace určen?

- Pro každého jednotlivce či organizaci, která chce zabezpečit svoje data a komunikaci proti zneužití cizí stranou
- Souhrn opatření a nastavení bezpečnostní politiky ochrání každý subjekt před ztrátou a zneužitím citlivých informací
- Aplikovaná opatření zajistí ochranu pomocí procesů a efektivních nástrojů

Výhody a cíle SOFO Bezpečné komunikace

- Aplikovatelnost na jakýkoliv subjekt bez rozdílu velikosti či oboru působnosti
- Kompletní analýza komunikačních kanálů a aktiv firmy
- Zabezpečení proti zneužití dat a nástroje pro bezpečnou komunikaci
- Nastavení postupů a nástrojů pro bezpečnou komunikaci také uvnitř firmy
- Aplikace šifrovacích komunikačních prostředků a datových nosičů
- Posouzení datového a energetického zálohování s ohledem na rizika a hrozby
- Důkladné školení a vzdělávání zaměstnanců a obchodních partnerů firmy
- Zázemí stabilní a důvěryhodné firmy
- Mezioborový tým profesionálních konzultantů s dlouholetou praxí a příslušnými certifikáty
- Možnost výhodného financování

Analýza současného stavu

- Analýza aktiv, komunikačních kanálů, bezpečnostních perimetrů a jejich ochrany
- Realizace penetračních testů infrastruktury
- Aplikace sociálního inženýrství
- Revize právních vztahů
- Identifikace kritických bodů komunikace a zabezpečení aktiv

Návrh procesů vztažených k životnímu cyklu dat a informací, jejich zpracování a archivaci

- Návrh topologie ICT infrastruktury
- Zohlednění individuálních požadavků zákazníka na dostupnost, mobilnost a modifikovatelnost informací a dat
- Vytvoření plánů vzdělávání v oblasti bezpečné komunikace

Podpora při implementaci navržených opatření

- Vedení projektového týmu zákazníka
- Technická podpora
- Legislativní podpora
- Vzdělávání

After case service

- Periodické testy
- Podpora uživatelů zákazníka (HELP-desk)
- Monitoring, odstraňování problémů
- Pravidelné vzdělávání a školení zaměstnanců kvalifikovanými lektory
- Podpora i pro Vaše obchodní partnery a dodavatele
- Minimální administrativní zátěž pro zákazníka

Bezpečnost dat

- Důraz na aktiva zákazníka
- Aplikace bezpečnostních opatření potřebné vyhovující úrovně
- Aplikace vhodného fyzického perimetru
- Právní opatření při nejčastějších situacích úniku dat a soubor pravidel, jak se legislativně bránit

Vzdělávání

- Bezpečné zacházení s aktivy a dodržování bezpečnostních opatření pro všechny zaměstnance
- Školení managementu a workshop, jak užívat šifrovací zařízení pro bezpečnou komunikaci
- Simulace modelových případů odposlechů a úniku informací a aplikace návrhů opatření
- Školení a vzdělávání pro Vaše obchodní partnery i dodavatele

Svěřte své ISMS profesionálům

- Tým kvalifikovaných konzultantů
- Proaktivní přístup
- Prověření dodavatelé bezpečnostního HW a SW

sofogroup®

CASE STUDY

Většina organizací investuje vysoké částky do fyzického zajištění svých dat pomocí ICT technologií a zabezpečovacích systémů.

Zapomíná při tom na nejvíce rizikový prvek, kterým jsou lidé.

A to zejména vlastní pracovníci a obchodní partneři.

Tyto hrozby si uvědomil i jeden z našich klientů, který se rozhodl zabezpečeit svoji firmu proti úniku informací a proškolit své zaměstnanace pro správné zacházení s ciltivými daty.

Společnost je z oboru stavebnictví, kde je velmi silné konkurenční prostředí, a tedy i velká možnost zneužití citlivých firemních dat.

Řešení pro našeho zákazníka se zaměřilo na komplexní ochranu aktiv tak, aby nebyl opomenut žádný proces ani zdroj.

Případová studie

Vedení významné stavební společnosti začalo vnímat oblast bezpečnosti informací jako velmi významnou až poté, co došlo k úniku interních dat ke konkurenci, jehož výsledkem byla ztráta nejedné rozjednané zakázky. Dlouhodobá spolupráce se společností SOFO Group a.s. v oblasti procesního poradenství byla na základě tohoto incidentu rozšířena i do oblasti bezpečnosti informací, kdy prvním realizovaným krokem byla důsledná analýza rizik jak technických, tak sociálně - organizačně - personálních. Analýzu provedl tým konzultantů SOFO Group a.s., ve kterém byli zastoupeni jak odborníci na IT, tak na systémy řízení, ale i zkušení personalisté.

Tým využil interní metodiku hodnocení rizik společnosti SOFO Group a.s. založenou na kvalitativních metodách a na základě výsledků analýzy rizik sestavil akční plán, který řešil nejpalčivější identifikované rizikové oblasti. Mezi významnými oblastmi s neřešenými riziky byly zejména:

- dostupnost citlivých informací pouze oprávněným osobám a pouze ve správný čas,
- principy interní komunikace (tedy mezi kterými osobami a jakými komunikačními kanály docházelo k výměně informací),
- externí komunikace s významnými partnery a nevhodně zvolené komunikační nástroje,
- nevhodně nastavená pravidla práce s papírovými dokumenty,
- neřešená technická strana ICT, tedy nedostatečně nastavená pravidla síťového provozu a oprávnění k serverovým aktivům.

V akčním plánu tým sumarizoval navržená opatření dle termínové a finanční náročnosti implementace a následně ve spolupráci s interními ICT pracovníky zákazníka opatření začal implementovat. Velká část úsilí byla věnována i správnému nastavení monitoringu efektivity nasazených nástrojů.

První fáze implementace byla ukončena po 2 měsících, kdy byla provedena nová analýza rizik, která potvrdila významné snížení míry rizika kompromitace dat a tedy opakování nemilé zkušenosti, která k realizaci projektu vedla.

Sídlo společnosti:
Plzeň

Hlavní předmět činnosti:
Stavební průmysl

Využitá služba:
SOFO BEZPEČNÁ KOMUNIKACE