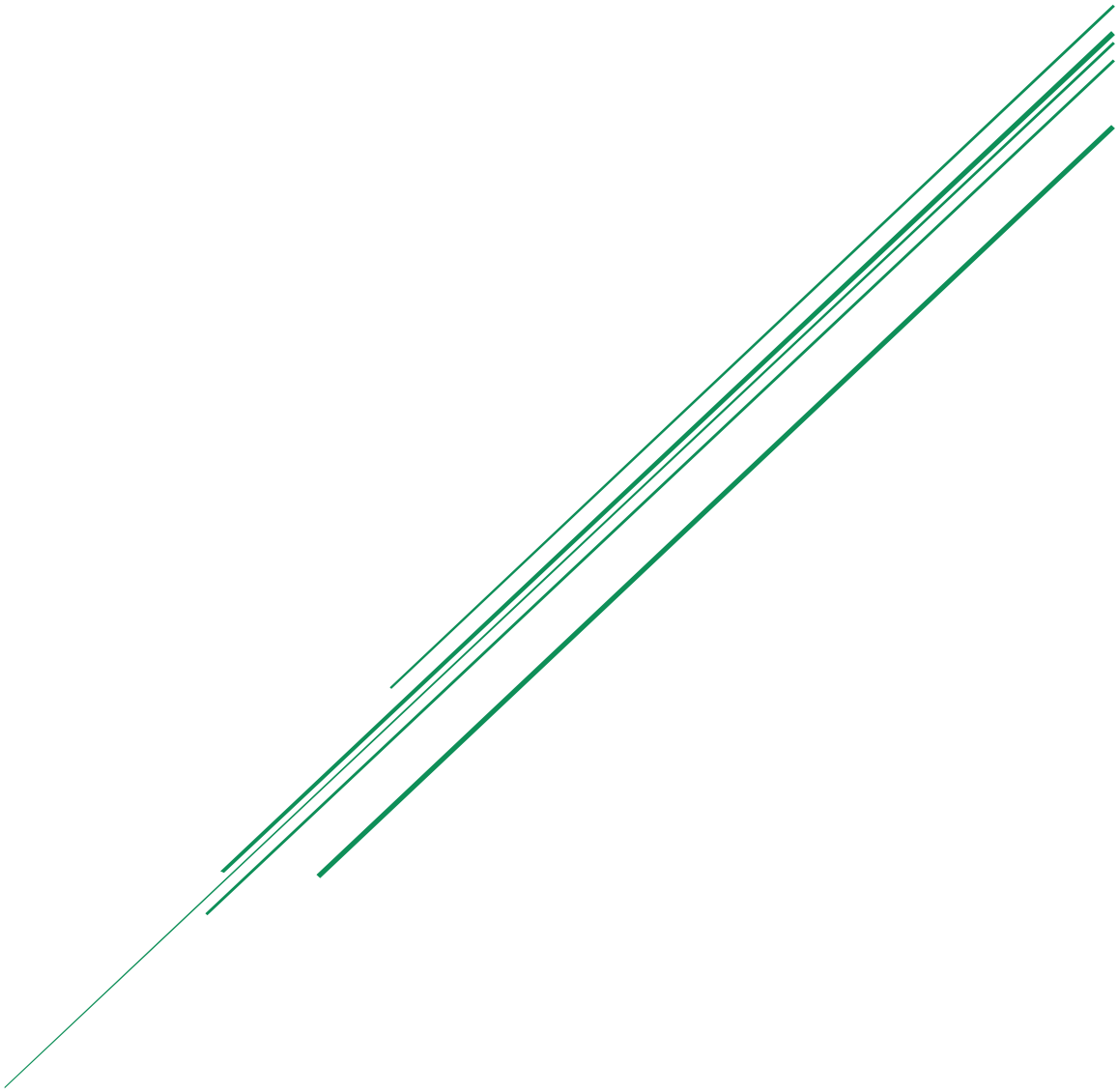
ROLKEN

Odolnost, spolehlivost a bezpečnost



Rolken s.r.o.
Nademlejnská 600/1
198 00 Praha 9

+420 228 224 645
hello@rolken.cz
rolken.cz

ROLKEN

Obsah

ROLKEN

V KOSTCE

15 let poskytujeme služby v oblasti kybernetické a IT bezpečnosti. Od jednoduchého skenu zranitelností (ve smyslu Vy nám řeknete, co potřebujete) po bezpečnostní transformaci (my Vám řekneme, co je možné a jak na to). Toto děláme pro **průmyslové**, **regulované** a **rozsáhlé organizace**.

Výsledkem naší práce je **zvýšená odolnost a spolehlivost** ve všem co děláte. Toho docílíme tak, že využíváme naši **expertízu a přenos know-how** z nejrůznějších odvětví.

Mluví za nás čísla: **97 %** projektů dodáváme **na čas,** v rozpočtu a projektovém vymezení, máme **99 % hodnocení kvality** a **98 %** zákaznickou **spokojenost**. S **90 %** klientů máme **dlouhodobé vztahy**.

Vznikli jsme v roce 2013 vyčleněním ze společnosti SUNFLOVV, která poskytovala služby informační bezpečností a bezpečnostního outsourcingu od roku 2007 bez jakýchkoliv vazeb na bezpečnostní produkty a dodavatele.

Nemáme žádné externí investory, společnost je vlastněná zaměstnanci a sídlíme v Praze. Od počátku si zakládáme na principech **vzdálené spolupráce** se silnou orientací na **technologie**, **inovace** a **automatizaci**.

ROLKEN

CO PRO VÁS MŮŽEME UDĚLAT

Nebyl to lepší motor, co umožnilo, aby vznikl rychlovlak Šinkansen, ale lepší brzdy, které umožnily využití síly motoru. Toto je filozofie, s jakou pracujeme – abyste mohli rychleji vpřed, musíte mít schopnost zabrzdit.

MANAŽMENT IT A OT AKTIV

Mít seznam aktiv, jako jsou systémy, aplikace, hardware, použitý firmware, je absolutní minimum pro řešení bezpečnosti. Nakonec, jak chcete chránit něco, o čem nevíte, že máte?

Pomůžeme Vám navrhnout proces, nastavit systém a automatizovat co jde, abyste měli všechny informace o aktivech a jejich stavu.

VHODNÉ POUŽITÍ

Pokud byste měli pro bezpečnost udělat jen jedinou věc, tak ať je to management aktiv. Bez aktuálního seznamu aktiv má každé další opatření či aktivita snížený nebo žádný efekt.

JAK POSTUPUJEME

Vytvoříme pro Vás seznam aktiv, hardware, software, aplikací, firmware, frameworků, zkrátka všeho, co najdeme. Zkombinujeme technická data ze sond a skenů s inventarizačními a dalšími „papírovými stopami“.

VÝSLEDEK

Získáte seznam všech aktiv, proces aktualizace informací o aktivech a systém pro kontinuální management aktiv.

INFORMAČNÍ EXPOZICE

Denně od vás proudí množství informací. Aktualizujete web, rozesíláte tiskové zprávy, řešíte problémy v mailových konferencích. Publikujete články a příspěvky na konference. Spolupracujete s univerzitami a studenti o vás píší diplomové práce. To vše je skvělé, jenom jestli nepomáháte i někomu, komu pomáhat nechcete. Nakonec, kdy jste naposledy zjišťovali, co najdete o Vás a vaší organizaci na uložto?

VHODNÉ POUŽITÍ

Když chcete vědět, co všechno o vás může zjistit útočník ještě předtím, než zaútočí.

ROLKEN

JAK POSTUPUJEME

Prověříme, co je o vás známo a získané informace zasadíme do kontextu. Spojíme vaše doménová jména, informace z WHOIS databáze a data ze sociálních sítí nebo prezentací. Tak, abyste poznali, jak vás vidí útočník.

VÝSLEDEK

Seznam veřejných informací a jejich bezpečnostní kontext. To vše z pohledu útočníka, jenž si dělá „domácí úkoly“.

HODNOCENÍ ZRANITELNOSTÍ

Nalezneme tolik zranitelností, kolik je možné a pomůžeme vám seřadit protiopatření podle vážnosti a dopadu.

VHODNÉ POUŽITÍ

Když už máte seznam aktiv a potřebujete seřazený seznam problémů s cílem opravit vše, co lze, a tak efektivně, jak je to jen možné.

JAK POSTUPUJEME

Otestujeme aktivum – server, aplikace, operační nebo řídicí systém – na přítomnost zranitelností. Samozřejmostí je seznam všech známých zranitelností, no nezůstaneme pouze při něm. Při hodnocení zranitelností hledáme i zranitelnosti, které nejsou veřejně známé nebo například jde o zranitelnosti v důsledku specifické konfigurace.

VÝSLEDEK

Seznam zranitelností s přiřazením vážnosti a návrhem protiopatření.

PENETRAČNÍ TESTY

Znát své silné a slabé stránky je důležité. Nalézt své slabé stránky je jeden z nejtěžších úkolů. A právě proto jsme tu my – vyhledávání slabých míst nás baví.

Pomůžeme Vám nalézt slabé stránky ve Vašich aplikacích, v infrastruktuře a v procesech, zdokumentujeme je a navrhneme protiopatření.

ROLKEN

VHODNÉ POUŽITÍ

Pokud máte seznam aktiv, zavedené skenování zranitelností a proces nápravy zjištění, je čas prověřit, jestli je možné dosáhnout konkrétního cíle, jako je například zcizení zákaznických dat, přístup k řídicímu systému nebo modifikace informací o platech.

JAK POSTUPUJEME

Na začátku si společně stanovíme 3 až 5 cílů. Testování na úrovni sítě probíhá dle NIST 800-115. Pro testování webových aplikací používáme metodiku OWASP. Nálezy hodnotíme pomocí Common Vulnerability Scoring System (CVSS).

VARIANTY

> TEST REAKCE NA INCIDENT

Zjistíte, jak vaše organizace a kolegové reagují na incident. Nebo, jestli ho vůbec zaznamenáte.

> EXTERNÍ PENETRAČNÍ TEST

Budete vědět o rizicích a hrozbách působících zvenku (při testu jsme mimo váš perimetr, napodobujeme někoho, kdo zatím nemá přístup do vaší sítě).

> INTERNÍ PENETRAČNÍ TEST

Budete vědět o rizicích a hrozbách uvnitř perimetru (při testu jsme uvnitř vašeho perimetru, napodobujeme například nespokojeného zaměstnance).

> PENETRAČNÍ TEST API

Prakticky každý systém používá nebo poskytuje rozhraní pro programátory. Prověříme, jak je na tom Vaše API. Někdy se nemá smysl útočit na aplikaci, když si lze celou databázi stáhnout jedním dotazem na API.

> PENETRAČNÍ TEST WEBOVÉ APLIKACE

Prověříme, jestli je možné eskalovat práva, získat data, která by neměla být veřejně přístupná nebo jiný definovaný cíl.

> PENETRAČNÍ TEST FYZICKÉ BEZPEČNOSTI

Prověříme fyzické bariéry (ploty, brány, vjezdy pro auta a další), zámky, možnost tail-gatingu a možnost obejití přístupového systému.

Zanalyzujeme kamerové systémy a alarmy i způsoby, jak jsou události zaznamenávány a vyhodnocovány.

V honbě za informacemi projdeme i vaše odpadky.

Nejjednodušší cesta, jak získat přístup kamkoli, je obléct si reflexní vestu a nést žebřík.

Počítáte a hodnotíte rizika, nasazujete různé bezpečnostní systémy anebo máte vybudované dohledové centrum.

A co když zjistíme, že dveře do serverovny nejsou uzamčené?

Máte nasazený přístupový systém, který využívá bezkontaktní karty? I na to jsme připraveni. Prověříme, jestli ho lze obejít, zkopírovat kartu nebo úplně obejít kontrolu.

Prověříme, jak systém zachází s citlivými daty jako jsou otisky prstů nebo dlaně, i jestli je možné systém obejít a získat neoprávněný přístup. A jako bonus budete mít podklad pro řešení GDPR.

A co třeba kamerový systém? Nelze ho obelstít nebo využít jako přestupný bod do vaší sítě? Prověříme, jak si na tom stojí, jestli ho nelze vyřadit a jestli nemá slepá místa.

> PENETRAČNÍ TEST IOT NEBO IIOT

Mít vše okamžitě dostupné – to máme rádi. To, že jde o vektor útoku, už méně. Prověříme, jak na tom stojí Vaše zařízení.

> PENETRAČNÍ TEST CLOUDOVÉHO PROSTŘEDÍ

Infrastruktura jako kód, cloudifikace, software jako služba, kontejnery, mikroservice – to všechno zrychluje vývoj. A přináší nové problémy. Otestujeme vše, co souvisí s cloudovým prostředím – od přístupových práv, volně dostupných dat až po logické chyby při designu prostředí.

VÝSLEDEK

Zpráva z penetračního testu je obvykle ve formě: ano, podařilo se nám dosáhnout zadaného cíle, nebo ne, nepodařilo se nám dosáhnout zadaného cíle a uvedeme všechna zjištění, kterých jsme si po cestě za určeným cílem všimli.

Neposkytneme Vám kompletní seznam zranitelností ani prioritizaci zjištění – na to máme sken zranitelností.

Sami neradi čteme desítky stran nudného textu. Proto naše zprávy píšeme tak, abychom mohli říct, že jde o literaturu faktu, která se čte jako thriller.

Samozřejmě obsahuje vše, co má dobrá zpráva mít – hodnocení, kvantifikaci, kvalifikaci a dopad.

Navíc nejde nám pouze o to, co nefunguje. Když nám něco zabrání v útoku, zdokumentujeme a pochválíme.

SOCIÁLNÍ INŽENÝRSTVÍ

Každý den se na Vás valí množství informací. Volají zákazníci, je potřeba zrevidovat materiál na poradu, z pojišťovny zaslali formulář, a navíc aktualizace systému, se kterou již druhý den volá IT. Jeden z těchto úkonů mohl být cíleným útokem, ale v denním shonu to nepoznáte.

Nebo víte, jak odlišit PDF s malware a objednávku od odběratele?

VHODNÉ POUŽITÍ

Řešit sociální inženýrství má smysl bez ohledu na bezpečnostní vyspělost. I když nemáte schopnost monitorovat odchozí síťový provoz nebo nemáte bezpečnostní dohledový centrum je dobré vyzkoušet, jak složité to bude útočník mít a jak Vaši kolegové reagují. I kdybyste nepřijali jediné protiopatření, získáte praktickou zkušenost a možná budete Vy a Vaši kolegové ostřílenější v tom, jak reagovat, když budete cílem skutečného útoku.

JAK POSTUPUJEME

Pokusíme se vám zaslat podvodný email, zavoláme vám, pošleme dopis, podvrhneme CD nebo USB, podáme žádost o informace. Hledáme hranici, kdy vaše systémy nebo procesy selžou. A řekneme vám i proč a jak si s tím poradit. Zkrátka cokoli, abyste věděli, co zabere, a co ne.

VÝSLEDEK

Přehled, jaké scénáře jsme zvažovali, které jsme vybrali a způsob, jak jsme postupovali. Samozřejmostí je tabulka s přehledem a početnostmi úspěchu a selhání a celkové hodnocení.

ČERVENÝ TÝM

Vytvoříme červený tým, jenž napodobuje skutečné útočníky s cílem vylepšit vaše obranné schopnosti. Červený tým můžeme vytvořit jako jednorázový nebo může fungovat kontinuálně (což doporučujeme). Základním pravidlem je, že červený tým nemá žádné omezení ohledně cílů a postupů. Samozřejmě při tom nebudeme unášet Vaše kolegy nebo ohrožovat provozuschopnost. Obrovskou výhodou kontinuální spolupráce je, že červený tým konstantně rozvíjí svoji znalost a přístup, a tyto znalosti přenáší na modrý tým. Na to, aby se modrý tým efektivně bránil, potřebuje, aby červený tým byl lepší než skuteční útočníci.

VHODNÉ POUŽITÍ

Když už máte pokryté základy, jako je správa aktiv, management zranitelností, a máte schopnost detekovat a reagovat na škodlivé nebo podezřelé chování ve vašem prostředí, je čas na červený tým. Jestli bojujete se základními opatřeními, doporučíme Vám jejich vyřešení ještě před využitím nebo vybudováním červeného týmu.

JAK POSTUPUJEME

Nejdřív se společně dohodneme na cílech, pak vytvoříme realistický útočný scénář, bez omezení jako jsou zakázané systémy nebo adresy, na které nesmíme přistupovat. Tyto hranice útočník nemá a je naším zájmem, aby byl scénář co nejrealističtější. Pak sesbíráme všechny informace, které půjde. Od fotografií vstupů až po sborník z konference, na kterou jste zapomněli. A teď už zůstává jenom útok provést, při tom napadneme systémy, pokusíme se překonat fyzickou bezpečnost nebo využijeme sociálního inženýrství. Na závěr zůstává vyhodnotit, jak útok probíhal a jestli jsme dosáhli cíle.

Jde nám o co nejvěrohodnější simulaci útoku. Proto nevymýšlíme scénáře jak z akčního filmu.

Jistě, prostřihnout optická vlákna poskytovatele a instalovat sondu nebo slanit do areálu lze. A víme, že to skoro zaručeně bude fungovat. Jenomže se nedozvíte nic, co už nevíte.

Proto provedeme více scénářů, upozorníme Vás na lehké cíle, a to vše tak, aby scénáře byly přiměřené z hlediska času a nákladů.

VÝSLEDEK

Jednorázové nebo pokračující schůzky s vaším modrým týmem, kde projdeme nálezy a způsob, jak vylepšit odolnost a stav bezpečnosti. Navíc připravíme sumarizaci a prezentaci pro Vaše nadřízené. Zpráva obsahuje technické detaily s postupem, jak zopakovat test krok za krokem. Součástí zprávy jsou taktická doporučení pro okamžitou nápravu a strategická doporučení pro dlouhodobé zlepšení.

HODNOCENÍ HROZEB

Posoudíme, jestli je hrozba, kterou jste obdrželi nebo detekovali důvěryhodná nebo ne. To, že existuje hrozba ještě nemusí znamenat, že ji musíte odstranit nebo investovat do její minimalizace.

VHODNÉ POUŽITÍ

Když se objeví nová hrozba nebo někdo deklaruje, že v budoucnosti provede útok.

JAK POSTUPUJEME

Naším cílem je zodpovědět na dotaz co se může pokazit. Vyhodnotíme kredibilitu a dopad potencionální hrozby spolu s pravděpodobností, že se hrozba stane realitou. Hrozby vyhodnocujeme prostřednictvím metodiky STRIDE, DREAD nebo attack tree podle toho, která se pro danou situaci hodí nejvíc.

VÝSLEDEK

Zpráva s analýzou a použitou metodikou pro objasnění, jak jsme došli k závěrům.

MODELOVÁNÍ HROZEB

Na rozdíl od hodnocení hrozeb je modelování hrozeb proces, kde identifikujeme všechny potencionální hrozby jako jsou strukturální problémy, scénáře, zranitelnosti, dostupné exploity, útočníci a dopady.

VHODNÉ POUŽITÍ

Modelování hrozeb je ideální provést v průběhu designu procesu a opakovat vždy po zásadních změnách. Na základní úrovni modelování hrozeb zachytí, zdokumentuje a vizualizuje vazby mezi útočníky, zranitelnostmi, útoky, protiopatřeními a dopady na byznys, organizaci nebo procesy ve vašem prostředí.

JAK POSTUPUJEME

Obvykle začínáme s útočníkem a stanoveným útočným scénářem a následně projdeme do zachycení toho, jaké zranitelnosti je možné zneužít, jaké exploity jsou dostupné, definujeme protiopatření, určíme jejich zastavovací účinek a vyčíslíme dopady do vašich činností.

Mimo expertů na jednotlivé bezpečnostní domény, je součástí našeho týmu vždy skupina expertů na oblast, ve které působíte.

Proto jsou součástí našich týmů i experti, například na řídicí systémy, SAP, výrobu, energetiku, procesní manažeři a další profese, které obvykle nenajdete v bezpečnostních firmách.

VÝSLEDEK

Dokumentace vstupních parametrů, metodiky vyhodnocení a popisu reziduálních rizik po nasazení opatření. Zpráva obsahuje taktické a strategické doporučení mimo samotného hodnocení hrozeb.

BEZPEČNOSTNÍ ARCHITEKTURA

Byli jsme jak při zavádění bezpečnostních řešení, při designu řídicích systémů, tak i při implementaci bezpečnosti do existujících systémů. Pracovali jsme v provozu, designovali datacentra, navrhovali sítě i implementovali aplikační bezpečnost.

To vše nám přineslo unikátní vhled do problematiky. A díky tomu Vám pomůžeme navrhnout bezpečnostní architekturu. Od definování cílů až po implementační plán, rozpočet a rozpad prací.

VHODNÉ POUŽITÍ

Dobrá doba na vytvoření bezpečnostní architektury je právě teď jestli ji již nemáte. A když už bezpečnostní architekturu máte a připravujete nasazení nových systémů, aplikací, procesů nebo jinou změnu, je dobré celou stávající bezpečnostní architekturu přehodnotit.

JAK POSTUPUJEME

Pokud máte bezpečnostní architekturu, zrevidujeme stávající stav, projdeme požadavky s vlastníky aktiv a jejich uživateli a zohledníme technický a bezpečnostní vývoj od doby vytvoření architektury až po současnost.

Pokud bezpečnostní architekturu nemáte, zaměříme se na to, co chcete jako organizace dosáhnout, jaký rozvoj ať již technický nebo organizační plánujete, a navrhneme, jak postupovat při rozvoji vašich systémů a aplikací tak, aby bezpečnost nebrzdila rozvoj.

VÝSLEDEK

Získáte katalog opatření, které je potřeba implementovat, diagram vztahů a principy, kterými se řídit. To vše ve vztahu k tomu, co děláte a jaké systémy, aplikace a procesy provozujete. S dobrou bezpečnostní architekturou je i výběr vhodných dodavatelů technologií mnohem jednodušší.

MANAGEMENT INCIDENTŮ

Pro řešení bezpečnostních incidentů poskytneme tým, nástroje i znalosti. To, že nemáte vytvořené bezpečnostní operační centrum a skupinu operátorů a analytiků, neznamená, že nemůžete na bezpečnostní incident reagovat.

VHODNÉ POUŽITÍ

Tady je to jednoduché – nejvhodnější využití managementu incidentů je v momentě, kdy detekujete, že se něco neobvyklého děje a získáte podezření, že jde o incident.

JAK POSTUPUJEME

Lze postupovat dvěma způsoby. Pokud máte vlastní bezpečnostní operační centrum, můžeme poskytnout pouze doplnění kompetence, například na aplikační bezpečnost, ICS/SCADA a/nebo specifický protokol. Pokud vlastní bezpečnostní operační centrum nemáte, můžeme poskytnout pomoc při řešení incidentu od začátku až do konce.

Na začátku určíme incident leadera a následně zjistíme, jestli se jedná o incident, jak je vážný a dohodneme další postup. Zjistíme, jestli došlo k napadení dalších aplikací a systémů nebo k úniku dat, a poskytneme technickou podporu vašim právníkům.

VÝSLEDEK

Incident neodčiníme, ale minimalizujeme škody a neutralizujeme dopady.

APLIKAČNÍ BEZPEČNOST

Nezáleží, jak dobře je zabezpečena infrastruktura, že jsou zavedena pravidla pro fyzickou bezpečnost nebo existuje detailní postup pro management incidentů, když lze stáhnou celou databázi klientů jedním dotazem do nezabezpečené aplikace.

VHODNÉ POUŽITÍ

Zabezpečovat aplikace je vhodné v každé fáze životního cyklu – před prvním nasazením, po nasazení nové verze nebo v průběhu rutinního provozu.

JAK POSTUPUJEME

Abychom si byli jistí, že je vše tak, jak má být, využijeme vše – od statické a dynamické analýzy přes fuzzing až po manuální testování.

VÝSLEDEK

Seznam nálezů, návrh protiopatření a dalších kroků ke zvýšení úrovně bezpečnosti.

KONZULTAČNÍ SLUŽBY

DŮVĚRYHODNÝ RÁDCE

Důvěryhodný rádce v bezpečnostním kontextu je někdo, kdo je Vám schopen říct, na základě vaší bezpečnostní vyspělosti a cílů, jaký přístup zvolit. Tato role je vázaná na konkrétní osobu a dlouhodobou spolupráci.

PLÁNOVÁNÍ, VÝBĚR DODAVATELE, OPONENTURA

Pokud jste se rozhodli implementovat průmyslové firewally se stavovou deep packet inspection (DPI), jednosměrnými bezpečnostními bránami (datové diody), šifrovací technologií na vrstvě 2-4, intrusion detection and prevention systems (IDS/IPS) nebo security incident and event monitoring (SIEM), jsme tady, abychom Vám pomohli. Budeme Vašimi konzultanty v průběhu plánovací fáze, pomůžeme Vám s implementací nebo poskytneme oponenturu dodavatelům.

ROLKEN

MANIFEST

Jsme dost malí na **butikový přístup,** ale dost zkušení na **jakoukoliv velikost projektu**. Navíc za roky, které se pohybujeme v byznysu, jsme si vytvořili širokou síť vývojářů, byznys a datových analytiků a dalších expertů, kterou umíme využít pro úspěch projektu.

Oceňujeme **dlouhodobé vztahy** – jak na straně kolegů, tak i na straně klientů a věříme, že tyto vztahy jsou nejlepším ukazatelem naší práce.

Víme, že čas je nejvzácnější komodita, kterou máme. Svůj čas si vážíme a přesně proto si vážíme i čas všech ostatních – proto **dodržujeme deadliny a termíny**.

Dobří přátelé **neporušují dohody**. Proto Vám nebudeme malovat vše na růžovo, ale když se na něčem domluvíme, tak dohodu dodržíme.

Jsme **otevření** – problémy pojmenujeme bez vytáček, ale slušně. Takto komunikujeme mezi sebou a budeme se tak bavit i s Vámi.

Nemyslíme si, že genialita a zručnosti nahradí nedostatek komunikačních schopností. I když vytvoříme sebegeniálnější řešení, nikdy nevznikne, pokud ho nedokážeme vysvětlit. Proto si zakládáme na **naslouchání a jasné řeči**.

Nebojíme se **přiznat chybu**. Jestli uděláme při práci chybu, napravíme ji a nehledíme na čas, který při tom strávíme. Protože nám na dobrém jménu záleží.

Rozumíme různým oblastem, ale nenecháváme se zaslepit jejich hranicemi. Při práci se inspirujeme i v jiných odvětvích, protože věříme, že **nejlepší věci vznikají na rozmezí různých oborů**.

A na konec – s námi **nebudete v kontaktu s account manažéry nebo sales**. Jednoduše proto, že nikoho takového nemáme. Každý projekt si vede přímo ten, kdo na něm bude pracovat.

ROLKEN

KONTAKTNÍ A PRÁVNÍ INFORMACE

Kontaktní údaje

+420 228 224 645

hello@rolken.cz

Korespondenční adresa

Rolken s.r.o.

Salmovská 1534/11

12000 Praha 2, Nové Město

Česká republika

Fakturační údaje

Rolken s.r.o.
Nademlejnská 600/1
198 00 Praha
Česká Republika

IČ: 02155176
IČ DPH: CZ0215517
DUNS: 361438111

Jsme registrovaní u Městského soudu v Praze, spisová značka C 216078.