OCHRANA KRITICKÉ INFRASTRUKTURY: jak mohou pomáhat vyspělá videořešení

Proč vieo hraje významnou roli pro udržení infrastruktury v chodu

MAKE THE WORLD SEE

milestone

Úlohou technologie je ochrana kritické infrastruktury

Již samotný pojem „kritická infrastruktura“ vypovídá o tom, nakolik lidská společenství spoléhají na životně důležité obslužné sítě, které udržují v bezproblémovém chodu naše dodávky energie a vody, náš finanční systém, komunikaci a dopravu.

Bez tekoucí vody bychom brzy skončili „na suchu“. Nucená přestávka v řízení dopravy dokáže paralyzovat celá města. A narušení obranných systémů zanechá zemi v extrémně zranitelném stavu.

Proto je ochrana kritické infrastruktury tak nesmírně důležitá – na fyzické i digitální úrovni. A tyto dvě úrovně spolu úzce souvisí. Ačkoli stále častěji dochází ke kybernetickým útokům, původ takového útoku bývá fyzický – může jím být například fyzické narušení nějaké vnější ochranné bariéry. Ochranou hmotných statků své firmy posílíte zabezpečení celého vašeho provozu. Ochráníte také zaměstnance na pracovišti, neboť zneužití skutečných slabin může mít za následek vyřazení bezpečnostního systému a ohrožení vašeho personálu.

To je také příčinou rapidního růstu trhu zaměřeného na ochranu kritické infrastruktury. Podle předpovědí má jeho hodnota do roku 2025 vzrůst na 108,57 miliard dolarů, a to z hodnoty 71,83 miliard zaznamenané v roce 2019. Kritická infrastruktura jakožto páteř moderní společnosti (a také ekonomiky, bezpečnostních složek a zdravotnictví) je atraktivním cílem útoku. Jakékoli přerušení jejího provozu může být otázkou života a smrti. Když ve Spojeném království na Nový rok došlo k pětihodinové havárii počítačového vybavení londýnské záchranné služby a její personál byl odkázán na tužku a papír, přímým následkem této nehody byla prokazatelně smrt nejméně jednoho pacienta. Vzhledem k časové naléhavosti 999 dalších zásahů ve stejný den jich však pravděpodobně bylo mnohem více.

Nelze opomíjet ani rozsah možných následků – síťové útoky na ukrajinský energetický systém v letech 2015 a 2016 ovlivnily život statisíců ukrajinských občanů. Při výpadku proudu v roce 2016 postrádaly firmy a domácnosti pětinu obvykle dodávané energie, a lidé proto zůstávali uvězněni ve výtazích, provoz firem se zcela zastavil a domy byly bez elektřiny. Když došlo k narušení hlavního vedení vysokého napětí na severu Německa, vedlo to k všeobecnému „evropskému blackoutu“, který postihl země na celém kontinentu, od Chorvatska po Španělsko, Portugalsko, Maroko, Alžír a Tunis.

Evidentně se jedná o případy volající po ochraně kritické infrastruktury. A k dispozici je celá řada technologií k jejímu zajištění. Jsou tu však jedinečné okolnosti a rizika, na něž se vedoucí činitelé musí připravit.

> Jakékoli přerušení jejího provozu může být otázkou života a smrti.

Výzvy z hlediska kritické infrastruktury

Část rizika kolem kritické infrastruktury spočívá v obecně rozšířených hrozbách, jimž vlády a organizace musí čelit. Existují tři hlavní kategorie možných ohrožení kritické infrastruktury:

Přírodní hrozby
Sem patří zemětřesení, vlny tsunami, vulkanické erupce, hurikány, sesuvy půdy a požáry.

Lidské hrozby
Sem patří nepokoje a stávky, zásahy do systému, exploze a bombové útoky, loupeže, terorismus, finanční kriminalita a průmyslová špionáž.

Hrozby náhodné a technické povahy
Sem patří selhání či nehody infrastruktury a nebezpečných materiálů, výpadky rozvodné sítě, havárie vodovodního potrubí, selhání bezpečnostního systému a další následky chyb všeho druhu.

Každá z těchto kategorií vyžaduje specifický přístup k fyzickému a digitálnímu zabezpečení pracoviště a také zvážení nejlepšího přístupu k ochraně jeho personálu. Díky výdobytkům technologického pokroku (například tepelné detekci, umělé inteligenci (AI), rozpoznávání obličeje a robotice) je předcházení velkému množství nově vznikajících hrozeb naštěstí stále snazší.

Fyzické bezpečnostní hrozby

K narušení bezpečnosti přímo na pracovišti může dojít několika způsoby, ať už ze strany zaměstnanců, nebo vetřelců usilujících o poškození vašeho vybavení a překonání bezpečnostních opatření, vyřazení nějakého systému či odcizení vašich dat. Mnozí kyberútočníci využívají k páchání svých zločinů právě fyzických přístupových bodů.

Zabezpečení pracoviště proti vnějším hrozbám (včetně rizikově jednajících osob) vyžaduje zavedení několika bezpečnostních vrstev:

- Perimetrická ochrana
- Kontrola přístupu
- Nepřetržité inteligentní videomonitorování prostorů
- Firewally
- Šifrování
- Zabezpečení archivace, zpracování a uchování dat

Nepřetržité sledování provozu je pro bezpečnostní týmy kriticky důležité, ale může být poměrně komplexní kvůli různým okolnostem, jako je lokalita konkrétního pracoviště, nutnost správy mnoha těžko dostupných oblastí (například u podmořského potrubí) či potřeba práce na dálku.

Kyberbezpečnostní rizika

Průměrné celkové ztráty vznikající narušením datové bezpečnosti organizace dosahují ve většině sektorů 3,86 milionů dolarů, vyšší jsou však ve zdravotnictví (7,13 milionu) a v případě organizací působících v energetice (6,39 milionu). Tyto ztráty vznikají nutností uhradit finanční náklady na opravu škod způsobených při takovém průniku, snížením produktivity a nucenými odstávkami systému. Nezanedbatelná je rovněž ztráta důvěry a dobré pověsti, zvláště pokud narušení bezpečnosti ovlivní životy mnoha lidí, což je v případě kritické infrastruktury pravděpodobné.

Není tedy žádným překvapením, že se kyberbezpečnost stala nejvyšší prioritou firem i vlád. Evropská unie navíc nedávno zavedla směrnici NIS o bezpečnosti sítí a informací, první celoevropskou kyberbezpečnostní právní úpravu, která má zajistit adekvátní ochranu všech členských států a jejich připravenost na kybernetické útoky. To znamená, že veškeré evropské organizace v kritické infrastruktuře se musí touto směrnicí řídit a zavést postupy identifikace neznámých zařízení, mechanismy detekce akutních hrozeb, programy kontroly zranitelnosti a efektivní plány zvládání incidentů a reakce na ně.

Útoky na kritickou infrastrukturu jsou stále častější, v roce 2019 utrpělo celosvětově 56 % užitkových zařízení zaměřených na plyn, větrnou energii, vodu a solární energii alespoň jeden kyberútok s následkem odstávky či ztráty provozních dat. Celých 54 % vedoucích bezpečnostních činitelů organizací působících v kritické infrastruktuře očekává další útok v následujících 12 měsících. Riziko dále zvyšuje škodlivý software (malware) vyvíjený cíleně pro útoky na řídicí systémy kritické infrastruktury, například Stuxnet a Black Energy.

Kyberútoky jsou stále obávanější, neboť kritická infrastruktura je čím dál více napojena na internet. Zatímco dříve mohla být určitá zařízení, např. elektrárny, provozována jako „bezpečnější“ uzavřené systémy, nyní dochází k všeobecnému rozšíření „internetu věcí“ (Internet of Things, IoT), a roste proto pravděpodobnost zneužití těchto zařízení síťovými útočníky.

Například chytré elektroměry jsou nyní prověřovány jako závažné bezpečnostní riziko, neboť rozsáhlý útok jejich prostřednictvím by mohl vyvolat přepětí a nárazem ochromit elektrickou rozvodnou síť. K vyřazení elektrické sítě z provozu by postačila úprava hodnoty energie požadované sítí chytrých elektroměrů o pouhé 1 %.

Jak vysvětluje zpráva Cambridgeské univerzity, chytré elektroměry přinášejí „několik závažných bezpečnostních problémů“, jako je možnost narušení bezpečnosti zákaznických dat, potenciální ovlivnění naměřených hodnot a hrozba všeobecného výpadku elektrické sítě.

Vzhledem k velkému rozsahu škod, které selhání kritické infrastruktury může způsobit ve společenské, bezpečnostní a hospodářské sféře postiženého státu, se kritická infrastruktura stala přitažlivým cílem pro případné nepřátele či protihráče na státní úrovni. Tato okolnost organizace nutí k ještě komplexnější přípravě na očekávané útoky a uvádí je do globální politické nejistoty.

Organizace jsou navíc vystaveny dalšímu rostoucímu riziku, které s sebou přináší rychlý nárůst digitalizace v souvislosti s pandemií koronaviru. Tato pandemie urychlila technologický vývoj přibližně o 5 až 10 let. Vzhledem k přesunutí dalších služeb do online světa je zde nyní více zranitelných míst, jichž mohou síťoví útočníci využít.

Jak ochránit kritickou infrastrukturu

Aby vedoucí pracovníci dokázali ochránit jak fyzický, tak digitální majetek společnosti, musí se soustředit na zamezení přístupu vetřelců (online i offline) a na proaktivní monitorování a výstrahy, které udržují neustálou informovanost bezpečnostního týmu a upozorňují jej na všechna aktuální rizika.

Podle povahy konkrétního pracoviště a provozu (kde může být například nutný přehled o několika roztroušených oblastech či pracovištích, potrubních rozvodech a velkém množství vstupních a výstupních bodů) mohou být některé aspekty fyzického zabezpečení náročnější než jiné. Proto je vhodné provést celkový audit veškerých rizik, zranitelných míst a stávající infrastruktury celého vašeho provozu ještě před investicí do nové bezpečnostní strategie či technologického balíčku odpovídajícího vašim potřebám.

Technologie zvyšující bezpečnost

Chytré organizace používají k posílení svého fyzického zabezpečení i kyberbezpečnosti vyspělé video zabezpečení využívající analytických nástrojů a umělé inteligence (AI). Díky posilování dominantního tržního postavení AI a jejímu vývoji k větší sofistikovanosti je pravděpodobné, že její využití brzy pronikne do odvětví robotiky a dronů.

Umělá inteligence může organizacím pomoci porozumět typickému chování na pracovišti a vypozorovat případné odchylky, které mohou být příznakem pokusu o sabotáž či neoprávněný přístup. Na ty následně upozorní bezpečnostní týmy a vedení společnosti, čímž umožní jejich reakci dříve, než dojde ke vzniku jakýchkoli škod. AI je obdobně využívána také k monitorování typického používání systému a k identifikaci případných škodlivých aktivit či potenciálních slabin online.

Využití chytrých technologií může bezpečnostnímu týmu ušetřit velké množství běhání a stresu. Moderní perimetrické systémy a systémy kontroly přístupu lze pro ucelenější představu o dění na pracovišti integrovat s daty získanými z videozařízení. Přístup lze povolovat automaticky na základě zadání osobních údajů a rozpoznání obličeje nebo identifikační karty. Obdobným způsobem lze detekovat a ověřit také dodržování použití OOP (osobních ochranných pomůcek). Pracovníkovi, který se nevybavil vhodnou ochranou hlavy či bezpečnostní obuví, může být například zamítnut přístup do nebezpečné oblasti až do chvíle, kdy si potřebné vybavení obleče.

Díky použití AI spolu s pokročilou analýzou videa mohou být bezpečnostní týmy automaticky upozorňovány na neoprávněný vstup, nebezpečné či podezřelé chování nebo na cizí vozidla.

Tepelné snímání zase dokáže pohotově upozornit na oheň v objektu.

Bezpečnostní týmy mohou tímto způsobem v reálném čase dálkově monitorovat aktivitu na mnoha pracovištích, mohou snadno rozpoznat, kdo a co na daném pracovišti je, kde se na něm nachází a nakolik splňuje požadavky bezpečnostních předpisů. Jsou tedy vybaveny veškerými kriticky důležitými informacemi, které jim umožňují neprodlenou reakci na případné hrozby.

Aktuálně dostupné pokročilé technologie

Progresivně uvažující vedoucí mají k zabezpečení svých firem k dispozici celou řadu nástrojů:

Detekce neoprávněného vniknutí

Umožňuje automatické upozornění bezpečnostních týmů na potenciálně neoprávněný vstup či neobvyklý pohyb u hranic střeženého prostoru. Toto varování mohou spustit výstupy zvukových a video zařízení či senzorů.

Detekce tepla a ohně

Senzory umožňující detekci ohně a kamery pro tepelné snímání mohou týmu pomoci zjistit, zda se v prostoru s omezeným přístupem nenachází nějaká osoba, kterou by prozradila infračervená tepelná stopa vyzařovaná lidským tělem. Podobné je to v případě požáru na pracovišti, kdy je vedení firmy ihned upozorněno na neobvyklý a náhlý nárůst teploty, a může proto okamžitě jednat.

Kontrola přístupu

Systémy kontroly přístupu mohou být integrovány s výstupy zvukových a video zařízení pro automatické umožnění přístupu jednotlivých osob na základě jejich identifikačních údajů. Mohou snímat jejich odznak či identifikační kartu, rozpoznávat obličej či hlasový vzor nebo analyzovat poznávací značku vozidla, a ověřit tak shodu jejich identity s tou očekávanou.

Interní správa vozidel

Na pracovišti lze u přijíždějících a odjíždějících vozidel monitorovat nezvyklý či nebezpečný způsob jízdy, podezřelý náklad či neočekávaný identifikační údaj vozidla. Díky tomu může bezpečnostní tým získat lepší povědomí o vozidlech v objektu a provádět jejich další kontrolu. Funkci automatického rozpoznávání poznávacích značek (ANPR) je možné integrovat s kontrolou přístupu pro automatické umožnění vjezdu předem autorizovaných vozidel. V případě neoprávněného vjezdu ji lze použít také k přijetí následných opatření. Je rovněž možné identifikovat vozidla s nebezpečným nákladem, automaticky na ně upozornit přítomné zaměstnance a varovat je k větší opatrnosti v okolí těchto vozidel, nebo jim při průjezdu takových vozidel nařídit opuštění dotyčného prostoru.

Systém monitorování incidentů

Tento systém bude na základě přednastavených parametrů (např. detekce pádu osoby z výšky nebo kolize vozidla) neustále monitorovat výskyt případných nebezpečných událostí vyžadujících rychlou odezvu. To bezpečnostním týmům umožňuje běžnou práci na každodenních úkolech až do chvíle, kdy je systém upozorní, že někdo potřebuje jejich zásah.

Monitorované chování

Systém dokáže analýzou výstupů ze zvukových a video zařízení porozumět obvyklému průběhu událostí na pracovišti a odesílat varování při výskytu chování či situací, které tomuto obvyklému průběhu neodpovídají. Zvýšené hlasy, náhlé a prudké pohyby či kradmý průnik osoby do oblasti s omezeným přístupem – to vše lze detekovat a zaznamenat pro pozdější kontrolu vedením firmy.

> Bezpečnostní týmy budou mít lepší povědomí o vozidlech v objektu a mohou provést jejich další kontrolu

Aktuálně dostupné pokročilé technologie

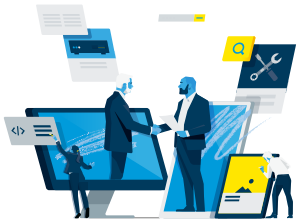
Progresivně uvažující vedoucí mají k zabezpečení svých firem k dispozici celou řadu nástrojů:

Centralizovaná kontrola

Nezbytným předpokladem správy více pracovišť je ústřední bod, jehož prostřednictvím mohou všichni odpovědní bezpečnostní pracovníci sledovat a monitorovat probíhající události. Uchovává také pořízené záznamy pro usnadnění pozdějšího vyšetřování či k umožnění analýzy za účelem zvýšení efektivity zabezpečení a provozních operací.

Detekce osobních ochranných pomůcek (OOP)

Systém dokáže skenováním zjišťovat použití vhodného ochranného vybavení u jednotlivých osob a připomenout jim stanovené požadavky, shledá-li jejich ochranu neadekvátní. Může se to týkat ochrany obličeje, například obličejových masek a ochranných brýlí, stejně jako ochranných přileb a bot, kombinéz, rukavic a ochranných štítů. Je-li tento systém integrován se systémem kontroly přístupu, může být určité osobě odepřen přístup do nebezpečné oblasti, dokud vhodné OOP nepoužije. Další inovace jsou patrné u chytrých přileb, které dokáží měřit takové faktory prostředí, jako je jeho vlhkost a teplota. Díky nim a postřehům z videovýstupů mohou vedoucí porozumět rizikům, která zaměstnanci na pracovišti podstupují, a aktivně je před takovými hrozbami chránit.



Automatizované sledování

Díky využití AI a počítačového pozorování mohou bezpečnostní týmy spoléhat na video zabezpečovací systém, který neustále monitoruje střežený prostor a upozorní na cokoli podezřelého. To je možné dovést ještě dál integrací robotiky a dronů, které mohou fyzicky patrolovat stanovenou oblast a odesílat nepřetržitý video výstup zpět do centralizovaného analytického systému. Tato technologie je zatím převážně v rané vývojové fázi, ale vyskytly se už první případy jejího použití. Zařízení Ring Always Home Cam je autonomní kamerový dron, který se po zjištění vloupání pohybuje po předem určených oblastech hlídané domácnosti. Má za úkol shromažďovat důkazy ve formě videa pro vyšetřující autority a umožňuje majitelům rychlou reakci na tyto hrozby. Algoritmus počítačového pozorování používají podobným způsobem také v americkém New Jersey k detekci nepovolených přechodů železniční trati, které jsou jednou z nejčastějších příčin zranění a úmrtí na železnici. Algoritmus se dokáže adaptovat na proměnlivé světelné a povětrnostní podmínky a mohl by být přizpůsoben pro přímé monitorování elektráren, těžebních plošin a podobných zařízení.

Zohlednění firemních procesů

Můžete investovat do té nejlepší dostupné fyzické a kybernetické technologie, ale ta nebude dokonale účinná, pokud nebude hrát bezpečnost ústřední roli také při tvorbě firemních procesů. Minimalizace veškerých hrozeb je podmíněna celofiremním společným přístupem.

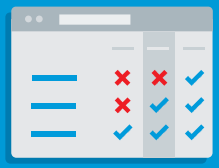
Spolupracujte ve fyzické i kybernetické oblasti
Je-li bezpečnostní oblast rozdělena tak, že jeden tým zajišťuje bezpečnost fyzických prostor a druhý se soustředí na kyberzabezpečení, může dojít k expozici zranitelných míst. Oba týmy musí proto komunikovat a pracovat na společném přístupu, jímž zajistí úspěšné pokrytí všech fyzických i kybernetických stanovišť. Svou hodnotu má také výměna vědomostí a zkušeností fungující mezi oběma týmy, takže si tým fyzického zabezpečení může osvojit například digitální dovednosti a znalosti aktuálních kybernetických hrozeb.

Prověřte si své externí partnery
Vše uvedené se vztahuje také na vaše externí partnery. Určitě není zbytečné vyhodnotit bezpečnostní protokoly vašich klientů, partnerů či dodavatelů i jejich zranitelnost. Narušení bezpečnosti bylo u 80 % organizací způsobeno některým z jejich dodavatelů. Přesto má však 77 % organizací o zabezpečení svých dodavatelů jen omezený (nebo žádný) přehled.

Porozumění lidskému faktoru
Je třeba brát v potaz také možnost lidského selhání. I sebelépe připravená a otestovaná bezpečnostní strategie může selhat, pokud některý ze zaměstnanců nevědomky otevře cestu útočníkům. Na každodenním provozu organizací se přitom často podílí velké množství osob, které neustále používají IT systémy a vstupují do přístupově omezených oblastí.

Každý člen organizace by měl porozumět bezpečnostním rizikům, která se pojí s jeho pracovní pozicí, a navíc také znát nejnovější hrozby. Pozornost věnujte zvláště tomu, co by mohl případný vetřelec získáním přístupu do určité oblasti získat – zaměstnanci mohou mít na svých stolech poznamenaná hesla nebo nechávat své počítače odemčené. Mohou se také stát obětí online útoků a e-mailových podvodů. K ukrajinskému výpadku elektrické sítě v roce 2015 došlo následkem útoku, který s využitím cíleného podvržení webového obsahu („spear-phishing“) šířil počítačový vir prostřednictvím e-mailových schránek zaměstnanců. Bez elektrického proudu následně zůstalo na 225 000 domácností.

Jedním z nejslabších článků zabezpečení bývají interní činitelé. Toto riziko lze částečně omezit zavedením detailního prověřování osobních profilů a referencí v průběhu přijímacího procesu. Týmy IT a týmy fyzického zabezpečení by ze stejných důvodů měly mít možnost monitorovat pohyb jednotlivce po pracovišti, stejně jako jeho přístupy k datům a použití různých zařízení.



Audit vaší stávající infrastruktury
Provádějte pravidelné hodnocení zavedených bezpečnostních procesů, technologií a informovanosti zaměstnanců, a zajistěte tak prevenci všech nejnovějších hrozeb. Udělejte si čas na poznání nových technologií i na porozumění tomu, jak tyto technologie mohou pomoci uspokojit vaše bezpečnostní potřeby. Sledujte zejména zastarávání vašeho vybavení, které se může stát zranitelným místem.

Belgická banka Argenta Bank se stala obětí „jackpotového útoku“ (spočívajícího v převzetí kontroly nad bankomatem tak, aby vydal celou zásobu hotovosti najednou), protože některé z jejích bankomatů byly zastaralé. Obdobně mohou síťoví útočníci či hackeři využít stejně zastaralého hardwarového vybavení a provozních modelů v tepelných či jaderných elektrárnách k získání přístupu do jejich systémů. Zastaralé a všemi zapomenuté zařízení ponechané v provozu bez jakýchkoli opravných aktualizací a s připojením k internetu může být vším, co případný útočník k získání neoprávněného přístupu potřebuje.

Nezapomínejte, že vaše bezpečnostní opatření musí obstát v boji s proměnlivými hrozbami a potenciálními vetřelci, kteří neustále hledají nové přístupové cesty do vašich systémů. Zabezpečení vaší organizace tudíž není jednorázovou akcí, ale nepřetržitým cyklem odhadů, investic, školení a vyhodnocování provozních výsledků.

Klíčové závěry

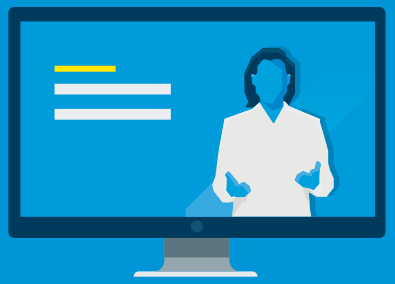
Současná bezpečnostní scéna je stále vyspělejší a stále více založená na datech. Firemní vedoucí mají k dispozici nepřeberné množství nástrojů k ochraně kritické infrastuktury, od inteligentního tepelného snímání a detekce vniknutí po kontrolu přístupu a dronovou technologii.

Klíčem k efektivní bezpečnostní strategii je nalezení té správné rovnováhy spolu s investicemi do technologií, které odpovídají vašim bezpečnostním cílům a nejnovějším hrozbám. Její zavádění vyžaduje také kolaborativní přístup v celé oblasti fyzického zabezpečení a kyberzabezpečení. Zásadně důležité je celofiremní vzdělávání zaměstnanců, neboť tu vždy bude lidská složka, s jejímž podílem na zranitelnosti je nutno počítat.

S pokračujícím rozvojem AI budou stále sofistikovanější také bezpečnostní technologie: budou přebírat další úlohy a umožní bezpečnostním týmům nepřetržitou informovanost o veškerém dění na pracovišti i online. Umělá inteligence nás uvede do nového věku inteligentního zabezpečení, který se bude automaticky přizpůsobovat vývoji bezpečnostních hrozeb – bude nepřetržitě chránit kritickou infrastrukturu a udržovat dokonalou informovanost firemních vedoucích o stávajícím vývoji, takže útoky jako Wanna Cry, vyřazení elektrické sítě na Ukrajině a „evropský blackout“ budou pouhými poznámkami pod čarou v historické kapitole o nezabezpečené éře.

Ochrana kritické infrastruktury

MAKE THE
WORLD SEE



Pokud byste se chtěli dozvědět více a hlouběji se ponořit do našich komunitních řešení, vyzkoušejte náš webinář:

Ochrana kritické infrastruktury

Po naskenování sledujte webinář

milestone

Milestone Systems A/S Headquarters
Banemarksvej 50 C
DK-2605 Brøndby
Dánsko
Telefon: +45 88 300 300

Nějaké dotazy?
S otázkami a dotazy se na nás obraťte zde.

Další informace najdete na webu:
milestonesys.com