Tok

PF 2021

N°02 - 2020

Volnou cestu novým rokem přeje všem **K-net**

BEZPEČNOST V HYBRIDNÍM SVĚTĚ 2

ZPRAVODAJ SPOLEČNOSTI K-NET

Dámy a pánové, vážení obchodní přátelé, milí čtenáři,

když jsme na sklonku léta připravovali minulé číslo časopisu Login, těšili jsme se na společný 16. Zákaznický den. V té době jsme ještě netušili, jak moc covid-19 ovlivní zdraví a životy mnoha lidí v naší zemi a opět pozastaví ekonomiku.

I my jsme nakonec museli Zákaznický den převést do on-line podoby a osobní setkání jsme nahradili sérií odborných přednášek na dálku. Spoustu energie jsme napřeli na pomoc zákazníkům s on-line komunikací. Hodně jsme se věnovali školám, se kterými úzce spolupracujeme už devět let díky historické Výzvě 51. Pomáhali jsme jim hlavně s tím, jak pracovat s nástroji Microsoft či Google. Například náš webinář pro školy na téma novinky v Microsoft Teams sledovalo více než 700 účastníků! Díky této intenzivní práci jsme se stali Microsoft in Education Global Training partnerem. Velmi nás to těší a současně to potvrzuje, že K-net umí nejen dodávat a spravovat IT technologie, ale také učit, jak je efektivně používat.

V minulém čísle Loginu jsme se zaměřili na kyberbezpečnost v hybridním světě. Je to opravdu velké téma dnešní doby i budoucnosti, proto v něm pokračujeme a podruhé mu věnujeme i celou manažerskou přílohu. Také vám nabízíme pohled na to, jak se nám podařilo provázat tři aktuálně řešené projekty a využít dotace z evropských zdrojů v oblasti IT, energetické soběstačnosti, fotovoltaiky a elektromobility.

Rok 2021 je pro nás jednou velkou neznámou. Nikdo nevíme, zda nás čeká klidná nebo naopak hektická doba. Přeji nám všem, abychom dokázali rozpoznat a využít vše dobré, co jsme se naučili v letošním, zcela výjimečném roce 2020. Abychom pracovali a komunikovali on-line, ale současně se neuzavřeli ve virtuálním světě, nadále si všímali přírody a všeho živého kolem nás.

Přeji vám dobrý rok 2021 a inspirativní čtení! Log in!

Ing. Tomáš Knettig
za tým K-net

ÚSPĚŠNÉ **POKRAČOVÁNÍ WEBINÁŘŮ** PRO ŠKOLY

O podzimní školení byl rekordní zájem.

Vývojové týmy společností Microsoft a Google usilovně pracují na zdokonalování svých technologií, které co nejvíce usnadňují práci pedagogům i žákům v této nelehké době. Proto jsme školám na začátku školního roku nabídli další dva webináře na téma *novinky v aplikacích vhodných pro distanční školní výuku*. Ve spolupráci s Microsoftem jsme pořádali webinář Novinky v MS Teams, o týden později jsme předvedli Novinky Google pro vzdělávání.

Velká obliba a zároveň potřeba těchto nástrojů u pedagogů způsobila až nečekaný ohlas našich webinářů. Zpráva o jejich pořádání prolétla na sociálních sítích jako lavina. Když se počet registrovaných blížil ke 300 posluchačům, museli jsme požádat Microsoft o vytvoření tzv. živé události, která jediná byla v době konání webináře schopna pojmout více jak 300 připojení. V čase pořádání webináře o novinkách v Teams chybělo 10 lidí, abychom dosáhli hranice 1000 registrovaných! Samotného webináře se pak zúčastnilo na 700 osob. Druhého webináře se zúčastnilo cca 300 lidí, což může být indikátorem toho, že Google Classroom není na českých školách tak populární jako Teams.

Těší nás, že jsme takto úspěšně navázali na jarní řadu webinářů pro školy a že jsme mohli pomoci pedagogům zvládnout výuku na dálku. Ze všech našich webinářů jsou pořízeny záznamy, které jsou umístěny na našem YouTube kanálu.

Sledujte naše akce
k.k-net.cz/akce-a-udalosti

K-NET SE STAL **PARTNEREM** MICROSOFTU VE VZDĚLÁVÁNÍ

Snažíme se stále zlepšovat naše služby pro školy.

Úzká spolupráce s Microsoftem v propagaci vzdělávací aplikace Microsoft Teams a nespočetné hodiny školení pedagogů na školách napříč Českou republikou našimi IT lektory přinesla K-netu povýšení na registrovaného partnera společnosti Microsoft ve vzdělávání s titulem *Microsoft in Education Global Training Partner*. Jsme teprve druhou čistě českou společností, která dosáhla na toto partnerství.

Microsoft in Education Global Training Partner
Microsoft

Vzdělání je jednou z významných oblastí, které se Microsoft věnuje. Bezplatně poskytuje školám Office 365 včetně aplikace MS Teams. Výzkum ukazuje, že inovace a technologie ve vzdělávání jsou klíčovými faktory, které vedou studenty k tomu, aby byli připraveni na budoucnost. Program Microsoft Global Training Partner každoročně propojuje Microsoft partnery s tisíci vzdělávacími organizacemi a pedagogickými pracovníky z celého světa – pomáhá jim co nejlépe využívat technologii pro výuku a učení, ať jsou kdekoli. Jsme hrdí, že spolu s vámi vzděláváme mladé lidi pro úspěšnou budoucnost – jejich i České republiky.

Další novinky na
novinky.k-net.cz

En | *Second issue of Login in 2020 continues with topic of cyber security as it is an important concern of now and in the future to come. During the whole COVID-19 crisis K-net has been helping schools across the Czech Republic with implementation of distant learning. In October we experienced a major success of 700 people attending our live webinar about new features in Microsoft Teams. Our endeavor earned us an important partnership with Microsoft as their Global Training Partner in Education. This puts us in an even better position to help many Czech schools realize the potential of modern technology in education.*

16. ZÁKAZNICKÝ DEN

Bezpečnost v hybridním světě

Číslo 16 je v numerologii symbolem pro zhroucení plánů – značí pochyby, nejistotu a pomíjivost světa. A jelikož právě šestnáctku nesl náš letošní Zákaznický den, máme za to, že něco na tom opravdu může být. Naše původní a pečlivé naplánování akce se totiž zcela zhroutilo. Zato však vzniklo nové „hybridní" spojení s vámi formou virtuální série workshopů, které jsme zrealizovali za pomoci našich partnerů. A tak se letošní Zákaznický den stal neplánovaně naším úplně prvním virtuálním Zákaznickým dnem, jehož uskutečnění bylo pro celý marketingový tým zajímavou výzvou.

Máme rádi změny a ač se těšíme, až se zase budeme potkávat osobně, on-line forma měla i své výhody. Pro naše účastníky přinesla nejen možnost absolvovat workshopy z pohodlí svého domova či kanceláře, ale také jsme měli možnost věnovat se tématům detailněji, předvést více názorných ukázek a celkově se vícekrát potkat.

Naše prvotina, která vznikla kvůli COVID-19, letos propojila nejen naše zákazníky, ale i další účastníky se zájmem o přednášky, jež se nesly v duchu tématu *Bezpečnost v hybridním světě*. Slovo bezpečnost má mnohem větší význam než před pandemií. Díky ní si lidé začínají uvědomovat, že bezpečnost je důležitá ve všech sektorech a dnes hlavně v IT. Kdyby v pandemické situaci zkolabovaly nemocnice, veřejné instituce či firmy, protože neustály kybernetický útok, jaký by to mělo následek? Kolik lidí by doplatilo na nezajištění této bezpečnosti? Netroufneme si toto číslo ani odhadnout. A právě k zajištění informovanosti o bezpečnosti a hybridní práci nám přispěli generální partneři – společnosti Citrix, Forcepoint a Quest a také partneři Acunetix a Flowmon. Akce se konala pod záštitou Asociace malých a středních podniků a jejich projektu Rok malého podnikání 2020.

Podívejte se jaký byl 16. Zákaznický den

k.k-net.cz/16-zakaznicky-den

Zákaznický den tradičně zahájil Tomáš Knettig, jednatel společnosti K-net, tématem VIZE K-NET 2020+, co nám pandemie přinesla a odnesla a jaké výzvy nás dále čekají (některé z těchto vizí představujeme na poslední straně Loginu). Následně každé čtvrteční dopoledne se střídali přednášející s tématy bezpečnosti ve svých oblastech působení. Tomáš Poslušný z Prianta představil nástroj Questu, Enterprise Reporter, který hlídá práva a přístupy všech uživatelů k jednotlivým aplikacím a dokumentům definovaných v Active Directory. Jeho kolega Lukáš Židlický vysvětlil, jak webový skener Acunetix účinně odhalí zranitelnosti webových aplikací, které je třeba ošetřit před hackery. Miroslav Bajgar z Forcepointu ukázal, jak kvalitně a komplexně ochránit své prostředí v cloudu, s následnou praktickou ukázkou využití next generation firewallu v cloudu K-net, resp. infrastruktuře zákazníka. Vladimír Střálka a Roman Kapitán ze Citrixu nás seznámili s intuitivním a bezpečným prostředím digitálního pracoviště Citrix Workspace. To sdružuje všechny podnikové aplikace, dokumenty, virtuální desktopy a také obvyklé uživatelské úkony s podnikovými aplikacemi do jednotného prostředí. Jiří Krejčíř z Flowmonu se zaměřil na novinky v jejich technologii pro identifikaci a řešení síťových problémů, které se týkají především daleko příjemnějšího ovládání pro nespecialisty na danou oblast. Praktickou ukázku využití předvedli naši IT konzultanti v K-net Cloud. Závěrečná přednáška patřila třem praktickým ukázkám prevence a ochrany IT při haváriích či přírodních katastrofách, kterou je možné mít v K-net Cloud nebo ve vlastních datacentrech.

Těší nás, že touto netradiční formou jsme mohli zprostředkovat skvělé pomocníky pro bezpečnost informačních technologií široké veřejnosti. Záznamy webinářů můžete zhlédnout na našem YouTube kanálu. Jsme také rádi za zpětnou odezvu ve vyplněných dotaznících, jejichž respondentům jsme se revanšovali malým dárkem. Čím nás překvapí další Zákaznický den?

En | *K-net's annual Customers Day had its 16th anniversary, and this year was taking place online due to COVID-19 pandemics. In 7 separate webinars a topic of Security in Hybrid World was introduced by K-net as well as main partners Citrix, Forcepoint and Quest and partners Acunetix and Flowmon.*

Rok malého podnikání 2020

Fotovoltaický přístřešek pro auta v Brně

EVROPSKÉ PROJEKTY: SMYSLUPLNĚ VYNALOŽENÉ PENÍZE

K-net letos ukončil rozsáhlý tříletý projekt, kterým reagoval na rostoucí poptávku zákazníků po cloudových službách. Svoji záložní serverovnu v Olešnici na Moravě vybavil stejnými technologiemi, kterými disponují moderní datová centra. Nové serverové technologie a nové technologie zabezpečení jejich provozu tak umožní další rozšíření poskytovaných služeb jak zákazníkům, tak potřebám stále se rozvíjejícího dohledového a monitorovacího centra. Kromě toho K-net řešil i další podpůrné věci, související s provozem budovy a rozšířením vozového parku.

Akumulace energie, fotovoltaická elektrárna a elektromobily

„S modernizací datového centra vzrostly naše požadavky na dodávku elektrické energie. Olešnice je malé město, kde jsme se nemohli stoprocentně spolehnout na to, že nám místní podmínky (lokální trafostanice atd.) zaručí optimum energie, kterou při zvýšeném provozu potřebujeme. Proto jsme začali hledat nové možnosti, jak poskytovat naše služby i bez toho, že by fungovala lokální dodávka energie ze sítě," vysvětluje Tomáš Knettig.

Součástí projektu nového datového centra byla i kogenerační jednotka. Podmínky jejího reálného nasazení nás pak přivedly na myšlenku, že jestliže se chceme nadále chovat zodpovědně k našemu okolí (datové centrum je chlazeno primárně venkovním vzduchem), musíme omezit provoz kogenerační jednotky v letních a přechodových měsících, protože bychom museli mařit strojem vyvíjené nadbytečné teplo. Tak se zrodil projekt pod názvem „Akumulace energie, fotovoltaika a dobíjecí stanice pro společnost K-net", jehož cílem bylo dále posílit energetickou soběstačnost datového centra a výrazně minimalizovat ekologický dopad výroby energie. Bateriové úložiště je hlavním prvkem celé soustavy, která umožňuje optimální využití energie vyrobené fotovoltaickou elektrárnou, energie vyrobené kogenerační jednotkou a distribuci této energie pro potřeby datového centra a rychlonabíjecích stanic pro elektrovozidla. Současně šlo o to snížit provozní náklady spojené s nákupem elektrické energie. Projekt byl podpořen z evropských zdrojů částkou přes 2,7 milionu korun (80 % celkových způsobilých výdajů) a umožnil pořídit fotovoltaickou elektrárnu, bateriový systém na bázi lithia a dobíjecí stanici.


Bateriové úložiště v Brně

Taktéž z Operačního programu Podnikání a inovace pro konkurenceschopnost získal K-net dotaci ve výši přes 1,2 milionu korun (75 % celkových způsobilých výdajů) na pořízení tří elektromobilů včetně mobilních nabíjecích stanic. Ty umožňují dobití vozidla ze standardní třífázové zásuvky (3F 400V 16A) za pouhé 3,5 hodiny. Můžete tak elektrovozidlo nabít ze stejné zásuvky, jakou používáte například pro připojení cirkulárky. Tři nové vozy tak doplnily stávající vozový park, který do té doby již zahrnoval tři starší elektromobily a čtyři hybridní vozy. Rychlonabíjení se tak stalo důležitou součástí pohodlného užívání v případě, že všichni řidiči elektrických vozů se sejdou na pracovišti ve stejném čase.

„Přestože jednotlivé projekty na sebe navazovaly, nepostihli jsme při jejich přípravě všechny technologické vazby a dopady. Až ve chvíli, kdy tyto tři projekty ležely vedle sebe, jsme zjistili, že dává velký smysl, dokážeme-li vyrobenou energii nejenom ukládat, ale také distribuovat s minimálními ztrátami způsobenými převody mezi střídavou a stejnosměrnou složkou proudu při nabíjení našich elektrovozů. Dokonce jsme v tomto smyslu požádali o změnu projektu, přestože jsme věděli, že na toto rozšíření se již dotace nebude vztahovat a budeme muset tuto část zaplatit bez podpory," doplňuje Tomáš Knettig. Pro rychlonabíjení stejnosměrným proudem bylo nutné změnit koncepci bateriového úložiště; změnit jeho pracovní napětí, a tím i mírně navýšit kapacitu. V původním projektu nebylo v Brně počítáno s tak výkonným bateriovým úložištěm. Proto K-net zažádal o dotaci na pořízení stacionárního bateriového úložiště o kapacitě 33,6 kWh, které doplnilo stávající identické úložiště napojené na fotovoltaickou elektrárnu. Doplněné úložiště slouží k vyvažování špičkové zátěže elektrických příkonů a pro nabíjení elektrovozů poskytuje rychlonabíječce stejnosměrný proud bez dalšího měniče. Projekt byl podpořen částkou 319 400 korun z Operačního programu Podnikání a inovace pro konkurenceschopnost. „Najednou ta práce s energií dostala zcela jinou hodnotu," říká jednatel společnosti.

JSEM VELKÝM PŘÍZNIVCEM ELEKTROMOBILITY,

ŘÍKÁ V ROZHOVORU TOMÁŠ KNETTIG

Netajíte se už léta láskou k elektrickým vozům. Proč jste si je tak oblíbil?

Odpověď na tuto otázku má dvě roviny: strategickou a praktickou. Strategickou proto, že podle mého názoru vůbec není chybou, aby Česká republika byla méně závislá na dovozu ropy a naopak byla více soběstačnou zemí v oblasti výroby energií, ať už z jádra nebo z přírodních zdrojů. Po praktické stránce je ježdění elektromobilem skutečně jednoduché a opravdu velmi příjemné. Neznám žádnou nevýhodu, snad jen nutnost více plánovat cesty na delší vzdálenosti.

Kolik elektrovozů aktuálně K-net využívá?

Máme šest elektrických vozů a minulý týden jsme podepsali smlouvu na další čtyři – dvě referentská vozidla a dvě dodávky. Jsme rádi, že jsme mohli využít dotaci z evropského projektu na podporu elektromobility.

Další naše projekty podpořené EU na
k.k-net.cz/eu-projekty-a-rozvoj

Jaká je aktuální nabídka elektromobilů na českém trhu?

Zdánlivě to vypadá, že elektrovozů je na trhu dostatek, ale ve chvíli, kdy člověk hledá vůz pro určitý účel, tak je výběr přece jen omezený. Nicméně očekávám, že se to během dvou, tří let výrazně změní.

K-net propojil tři zajímavé myšlenky, které se týkají hospodaření s energií, fotovoltaiky a elektromobility, do jednoho funkčního celku. Můžete laicky vysvětlit, o co jde?

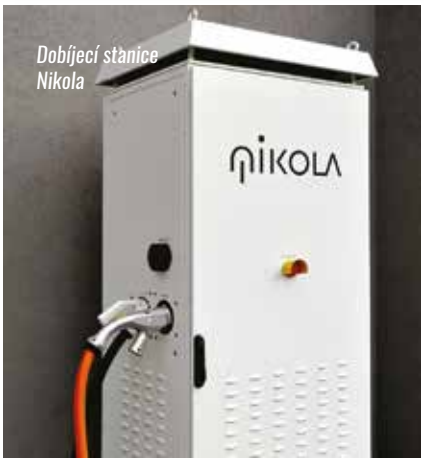
V podstatě jde o způsob, jak vyrobit a uchovat elektrickou energii, kterou nemusíte spotřebovat okamžitě, ale kterou si můžete uschovat a využít ji tehdy, kdy ji opravdu potřebujete. Představte si, že za letních horkých dnů získáte energii ze sluníčka, tu částečně spotřebujete na provoz svého datového centra a zbytek uložíte do akumulační baterie. A později tuto energii z baterie opět pošlete dál a využijete ji například k nabíjení elektromobilů. Zní to vcelku jednoduše, že? Ale ve skutečnosti jsme se hodně napřemýšleli nad tím, jak to v praxi udělat, aby takový model optimálně fungoval. Museli jsme například vyřešit, jak omezit velké ztráty, vznikající při převodech stejnosměrného proudu na střídavý a naopak, zakoupit větší bateriové úložiště nebo zajistit, aby nedošlo k přetížení přívodů elektrické energie při rychlonabíjení. Navíc v zimě je do tohoto procesu zapojena plynová kogenerační jednotka, takže z akumulační nádrže vytápíme celou nemovitost a zároveň jsou nabité baterie, které nám pomáhají zajistit elektrický provoz. Tento model je opravdu velmi funkční. Aby však dobře fungoval a křivka úspor byla optimální, je potřeba celý systém velmi dobře měřit, pozorovat a dolaďovat. K tomu využíváme naše vlastní produkty netGuard a netSense.

Co všechno vaše produkty hlídají a zjišťují?

Musím to vzít trochu zeširoka. Od roku 2010 opravdu intenzivně sbíráme a vyhodnocujeme data z výpočetní techniky o informačních technologiích. Průběžně jsme došli k poznání, že v případě selhání techniky nejsme schopni zhruba u poloviny případů identifikovat důvod kolapsu. Z toho vyplynulo, že musíme mít daleko více informací o vnějším prostředí, ve kterém technika funguje. Proto jsme vyvinuli produkt netSense.

V tuto chvíli nejenže sbíráme informace o tom, že běží sever, jaké má ovladače, kolik je místa na disku, jak jsou vytížené procesory, kolik dat protéká atd., ale také hlídáme, jaká je spotřeba energií, jaké proudy tam tečou, jaká je teplota v místnosti, jaká je tam vlhkost atd. Když jsme napočítali, kolik čidel bychom potřebovali na jednu serverovnu, došli jsme ke statisícovým částkám, takže jsme se pustili do výzkumu a vývoje vlastních čidel a vznikl netSense. Najednou vidíme nejen to, co dělají všechny technologie, ale jsme schopni rozkrýt, kde vznikl problém u cca 25-30 % dříve nevysvětlitelných odstávek. Například dohledáme, že nešla klimatizace, byla problematická dodávka elektřiny nebo v tom čase byl problém někde jinde. To všechno nyní můžeme pozorovat a podle toho upravovat procesy, aby technika lépe fungovala.

Elektromobil BMW i3



Dobíjecí stanice Nikola

En | *K-net finished 3 interconnected projects subsidized by the EU from the Operational Programme Enterprise and Innovations for Competitiveness. Thanks to the program K-net has both in Brno and Olešnice own photovoltaic power plants, battery storages, charging stations for electric vehicles and 3 new electric cars. These all contribute to minimizing K-net's carbon footprint, increasing its power independence needed for reliable operation of its cloud centers and saving of financial resources on energies.*

Jméno žadatele:
K-net Technical International Group, s.r.o.

EVROPSKÁ UNIE
Evropský fond pro regionální rozvoj
OP Podnikání a inovace
pro konkurenceschopnost

MINISTERSTVO PRŮMYSLU A OBCHODU

Všechny tři projekty byly podpořeny tímto programem:

OPERAČNÍ PROGRAM PODNIKÁNÍ A INOVACE PRO KONKURENCESCHOPNOST

NÁZEV PROJEKTU
Pořízení elektromobilů a nabíjecí stanice pro potřeby společnosti K-net Technical International Group, s.r.o.
Termín realizace
31. 5. 2017 – 31. 12. 2018
Způsobilé výdaje
1 622 474,00 Kč
Výše Dotace
1 216 855,50 Kč
(75 % celkových způsobilých výdajů)

NÁZEV PROJEKTU
Akumulace energie, fotovoltaika a dobíjecí stanice pro společnost K-net Technical International Group, s.r.o.
Termín realizace
31. 5. 2017 – 30. 9. 2019
Způsobilé výdaje
3 413 095,00 Kč
Výše Dotace
2 730 476,00 Kč
(80 % celkových způsobilých výdajů)

NÁZEV PROJEKTU
Pořízení bateriového uložiště k pokrytí odběrových špiček nabíjecí stanice na elektromobily společnosti.
Termín realizace
31. 05. 2019 – 31. 8. 2020
Způsobilé výdaje
399 250,00 Kč
Výše Dotace
319 400,00 Kč
(80 % celkových způsobilých výdajů)

NAPADL NÁS KRYPTOVIR

Zkušenost společnosti ATIS s reálnou hrozbou pro české firmy.

Kybernetická hrozba zvaná kryptovir neboli ransomware je v současné době hrozbou číslo 1 pro IT společností a organizací. Mimo medializovaných kauz nemocnice Benešov či OKD a dalších se tato „nákaza" bohužel nevyhnula ani významné české cestovní kanceláři ATIS.

Jak se kryptovir dostal do sítě, není přesně známo. Pravděpodobně šlo o závadný e-mail nebo nějakou nezjištěnou díru v systému. Toto se velmi těžko zpětně dohledává, pokud přijdete o data a přístup do systému. K nákaze došlo někdy před 8. 8. 2020 ransomwarem Phobos.C., k samotnému šifrování souborů potom v noci ze soboty 8. 8. na neděli 9. 8., kdy v neděli ráno byl systém nedostupný a téměř všechny soubory zašifrované. Došlo k napa-

dení devíti serverů z celkových třinácti, jeden neměl nastaveno žádné sdílení a byl mimo doménu, zbývající tři zachránil zálohovací software Acronis, který rozpoznal nestandardní chování a proces kryptování zastavil.

Poté, co došlo k vypnutí všech zařízení a odpojení serverů, se začal zjišťovat rozsah škod. Vzhledem k tomu, že kryptovir se šířil pravděpodobně přes sdílení souborů, napadl vše, co viděl v síti. Neunikly tomu ani zálohy, které byly zálohované na sdílené úložiště, i když byly pod speciálním administrátorským účtem mimo doménu. Téměř všechny servery byly nefunkční a nepřístupné. Jediné, co zůstalo funkční, byl naštěstí informační systém cestovní kanceláře, který je webový a běží v cloudu u dodavatele. Každopádně velkým problémem bylo to, že nebyly k dispozici žádné e-maily, dokumenty ani jiná data.

Hned v neděli se tedy začalo s opravnými pracemi ve spolupráci se společností K-net. Prvním krokem bylo najít v systému daný virus a ten ze systému odstranit. To se naštěstí podařilo celkem rychle pomocí antiviru ESET. Vzhledem k tomu, že nebyl zašifrovaný systém doménového serveru (Microsoft Active Directory) a terminálového serveru, podařilo se ještě během neděle nouzově zprovoznit chod kanceláře. Větším problémem byl e-mailový server, který bylo nutné instalovat celý od začátku včetně kompletní konfigurace. K úplnému zprovoznění došlo až v průběhu dalšího týdne, kdy uživatelům začala chodit nová pošta, ale starou poštu samozřejmě neměli k dispozici.

Vzhledem k tomu, že mnoho dalších dokumentů a systémů bylo neobnovitelných, začaly se paralelně zjišťovat další možnosti obnovy. Po konzultaci s antivirovou společností ESET bylo ověřeno na stránkách nomoreransom.org, že dekryptor k tomuto typu ransomware neexistuje a pravděpodobně nějakou dobu existovat nebude (pokud vůbec někdy). Došlo tedy k pokusu kontaktovat útočníka. Útočník požadoval cenu za dekryptování 1 bitcoin (v přepočtu asi 230 tisíc Kč v době incidentu). Po delší diskusi slevil na 0,5 bitcoinu. Po interní dohodě s jednateli společnosti mu byly tyto peníze odeslány. Výsledkem bylo bohužel obdržení kódu pouze k jednomu systému a za ty další požadoval další peníze (6800 USD). Toto už bylo pro společnost neakceptovatelné, a tedy s útočníkem diskuzi přerušila.

Dalším pokusem bylo kontaktování společností, které se profesionálně zabývají řešením následků po napadení kryptovirem. Osloveny byly společnosti beforecrypt.com a datarecovery.com. Jak se ale ukázalo, tyto společnosti žádné dekryptory nemají a jsou to pouze profesionální vyjednavači. Tedy za cenu například 3000 € vám zajistí odbornou komunikaci s útočníkem. Ručí za to, že útočník data dešifruje, ale v ceně samozřejmě není poplatek útočníkovi, a ten samozřejmě nejsou schopni dopředu sdělit. Reagují ale opravdu velice rychle a jako první krok posílají hned na proplacení svoji fakturu.

S ohledem na výše zjištěné informace bylo vedením společnosti rozhodnuto, že se do dalšího pokusu o obnovu dat nebude pouštět. Vše bylo zarchivováno v daném stavu a byl spuštěn postupný proces instalace nových systémů. Některé drobné systémy se ještě podařilo obnovit ze starších archivů, ale většinu bylo nutné zprovoznit a pořídit znovu.

Aktuálně se samozřejmě pracuje na kompletní změně zálohovací strategie. Zálohovací systém musí být zcela oddělen od produkční infrastruktury a zálohy nesmí být pro útočníka dostupné. Po těchto zkušenostech budou určitě vytvořeny minimálně 2 kopie různých záloh a minimálně jedna bude vytvářená na přenosné disky a odnášená mimo budovu. V řešení byla i záloha do Cloudu K-net, ale s ohledem na velké množství dat a stávající konektivitu společnosti to bude ještě realizováno starým způsobem na přenosné disky. Uvažovaným řešením je zálohovací systém Veeam nebo Nakivo. Zálohování by mělo být ideálně prováděno ze zálohovacího serveru či NAS, kde bude zálohovací SW instalován. Ten by měl zálohovat celé virtuální systémy přes rozhraní virtualizace bez toho, aby bylo v síti cokoli sdíleno.

Článek vznikl s laskavým svolením vedení ATIS, které umožnilo sdílet svou zkušenost jako varování ostatním.

> *Můj osobní závěr a rada pro všechny, kteří měli prozatím štěstí: Smířím se s tím, že budu znova napaden, ale už se nesmířím s tím, že nebudu kvalitně zálohovat; jedině se zálohou nedojdete k trpkému zjištění, že se zločinci se nevyjednává.*

Jiří Zahradník
IT, ATIS

Jak probíhala komunikace s útočníkem při vyjednávání? Čtěte na
k.k-net.cz/atis-a-kryptovir

En | *Czech travel agency ATIS has been attacked by a cryptovirus. Nearly all their data was crypted, including the backup. After paying 0.5 bitcoin the company was able to get decryptor to part of its data. However, they refused to pay more and couldn't decrypt the rest. This situation can be omitted with better backup strategy, keeping the backups separate from internal network and the internet.*

MORAVSKOSLEZSKÝ KRAJ **BEDLIVĚ STŘEŽÍ** SVÁ DATA A SYSTÉMY

Zdroj: Moravskoslezský kraj

V Moravskoslezském kraji žije na rozloze 5 427 km² více jak 1,2 milionu obyvatel. V kraji působí přes 58 tisíc firem. Krajský úřad Moravskoslezského kraje sám zřizuje přes 200 příspěvkových organizací. Cílem krajského úřadu je bezpečná elektronická komunikace mezi jednotlivými příspěvkovými organizacemi, zákazníky, partnery a občany. K tomu aktuálně využívá technologie Forcepoint NGFW a také Citrix ADC.

Do datových center a k informačním technologiím provozovaným na krajském úřadu dnes z internetu nepronikne ani pověstná myška, aniž by se o ní nevědělo a neměla to povolené. Příchozí i odchozí internetová komunikace je monitorována na několika úrovních a řízena moderními, profesionálními technologiemi. Patří mezi ně i dvojice Next Generation firewallů (NGFW) Forcepoint, konfigurovaných pro režim vysoké dostupnosti, které hlídají provoz na nižších vrstvách síťové architektury. Bezpečnost webových aplikací je zajištěna aplikačními firewally (WAF) Citrix ADC (dřívější označení Citrix NetScaler). Ty jsou provozovány také v režimu pro vysokou dostupnost, tedy v případě výpadku jednoho přebírá jeho funkci druhý.

PROJEKT MODERNIZACE FIREWALLOVÉHO CLUSTERU

Modernizaci dosavadního firewallového clusteru řešil krajský úřad veřejnou zakázkou v roce 2019. V této soutěži uspěl K-net s nabídkou výkonných technologií **Forcepoint NGFW**. Dodávka a implementace byla zahájena začátkem roku 2020. O tom, že nejde o jednoduchý projekt, svědčila skutečnost, že pro práci realizačních týmů krajského úřadu a K-netu bylo v časovém harmonogramu vyhrazeno více jak 5 měsíců. Během této doby musel být zpracován podrobný implementační projekt, popisující převod stávajícího stavu na nový, včetně harmonogramu, definice akceptačních kritérií a popisu možných rizik. Následovala vlastní dodávka a implementace, zaškolení správců, provedení akceptačních testů a vše bylo završeno zkušebním provozem v délce 6 týdnů. Povedlo se a od července 2020 běží technologie v rutinním provozu.

NĚKTERÉ PARAMETRY PROJEKTU:

- NGFW Forcepoint je nasazen v clusteru (soustavě) o dvou nodech (zařízeních), přičemž každý nod je umístěn v samostatné technologické místnosti. V rámci řešení jsou využívány virtuální firewally, kdy každý má v síti odlišnou roli:
  - ochrana Wi-Fi sítě,
  - směrování komunikace mezi interními sítěmi,
  - oddělení komunikace mezi interní a externí sítí,
- v rámci implementace byly přeneseny tisíce objektů a pravidel z konfigurace původního firewallového řešení,
- největší komunikační politika se sestávala z více než 2 500 pravidel.

Nad rámec původního řešení převzal Forcepoint další bezpečnostní funkci, kdy slouží jako webfilter, tedy jako nástroj omezující, které webové stránky mohou uživatelé navštěvovat.

PROJEKT ZABEZPEČENÍ INTERNETOVÉ KOMUNIKACE – WEB APLIKAČNÍ FIREWALL

O něco dříve, v roce 2018, řešil krajský úřad svůj záměr zvýšit bezpečnost internetové komunikace pořízením systému pro ochranu aplikací a informací dostupných z internetu, tedy web aplikačního firewallu (WAF).

K uskutečnění záměru využil projekt s názvem „Realizace bezpečnostních opatření podle zákona o kybernetické bezpečnosti“, realizovaný z výzvy č. 10 Integrovaného regionálního operačního programu (IROP), registrační číslo: CZ.06.3.05/0.0/0.0/15_011/0002011. Ve veřejné zakázce s názvem „Pořízení systému pro trvalou ochranu informací dostupných z vnější sítě před neoprávněnou činností, popřením provedených činností, kompromitací nebo neautorizovanou změnou“ uspěl K-net s nabídkou technologií **Citrix ADC** (dříve Citrix NetScaler).

I v tomto případě musela být nejdříve provedena důkladná příprava projektu. Vzhledem k rozsahu implementačních prací bylo vyhrazeno období ještě delší než v případě nasazení NGFW firewallů. Nicméně vše se podařilo zvládnout a v dubnu 2019 byl projekt předán do rutinního provozu.

V RÁMCI PROJEKTU:

- byla implementována funkce aplikačního firewallu na vybrané weby a webové aplikace krajského úřadu,
- byly použity další funkčnosti Citrix ADC jako load balancing, které souvisí s optimalizací rozložení provozní zátěže na jednotlivé webové servery,
- v rámci analýzy bylo testováno a bezpečnostně optimalizováno cca 150 webových stránek, aplikací nebo serverů.

V současné době krajský úřad nadále rozšiřuje počet chráněných webů a webových aplikací. V dnešní nelehké době využívá i další funkcionalitu Citrix ADC, a to SSL VPN pro mobilní uživatele.

> *„Realizace projektu nám přinesla zvýšené možnosti nastavení, vyhodnocování a analýzy bezpečnostních zásad a politik v porovnání s předchozí provozovanou technologií. Do budoucna nám nový systém umožní plnit zvyšující se nároky na kybernetickou bezpečnost a ochranu informací.*
>
> **Ing. Pavel Žák**, bezpečnostní manažer Krajského úřadu Moravskoslezského kraje

EVROPSKÁ UNIE
Evropský fond pro regionální rozvoj
Integrovaný regionální operační program

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

Moravskoslezský kraj

En | *Moravian-Silesian Region uses Forcepoint NGFW and Citrix ADC to keep their office secure. Forcepoint protects their network from harmful communication and serves also as a webfilter. Citrix protects their more than 150 web portals, applications, and servers and the project was subsidized by the EU. K-net helped with implementation of both.*

Přečtěte si další reference na
k.k-net.cz/reference

VIZE PRO ROK 2021 ANEB TRENDY PO ČESKU NEBO ANGLICKU?

Letošní Zákaznický den zahájil Tomáš Knettig tématem vize a trendy. V úvodu svého vystoupení udělal malý experiment: zadal do vyhledávače Google slovo „trendy“ anglicky a česky. A světě div se! Výsledky byly zcela odlišné. Zatímco pod anglickým slovem „trends“ se objevily odkazy technologického rázu, v češtině se pod „trendy“ zobrazila spousta oblečení. Trendy po česku byly spojeny hlavně s módou a tím, co módního se nosí. Vezměme to tedy spíše po anglicku. O čem se zřejmě bude v IT diskutovat v blízké budoucnosti?

ON-LINE KOMUNIKACE

Už nebude jen nouzovým řešením nebo výsadou určité firemní klientely, nýbrž běžnou součástí každodenní praxe. Videokonference se stanou nástrojem pro denní použití. „Vyladění“ komunikačních nástrojů bude úkolem pro výrobce, aby uživatelé získali co nejvíce užitečné a přívětivé komunikační prostředí. S tím bude souviset i potřeba edukace uživatelů. Dá se očekávat, že i příští rok se ještě budeme potýkat s dopady covidových opatření, takže bude pokračovat obrovský tlak na internet, jeho výkon a všechno s ním související. Myslíme si, že na on-line komunikaci budou muset přejít i organizace, které ji dosud nevyužívaly nebo se jí bránily.

BEZPEČNOST DAT

Zatímco přenos dat na dálku dramaticky vzrůstá, ne všechny firmy a organizace jsou na takový boom připraveny z hlediska bezpečnosti a ochrany dat. Většina zařízení ve standardních podmínkách je bezpečná, ovšem neplatí to v případě použití hrubé síly. V současné době probíhá velká část útoků metodou, kdy útočník zařízení přetíží, a tím ho vyřadí z provozu. Je třeba si uvědomit, že útoky nejsou vždy vedeny nějakým šikovným hackerem, ale plošně umělou inteligencí. S příchodem bitcoinu jsme svědky toho, že byly celosvětově vyvinuty neuvěřitelně silné systémy na výpočet šifer a současně vzrostlo nebezpečí, že tyto systémy budou použity pro dešifrování, tedy pro překonání šifry = podpisu, hesla atd.

VLASTNÍ SERVEROVNA NEBO EXTERNÍ CLOUD? MOŽNÁ „HYBRIDNÍ ŘEŠENÍ“

Provozní bezpečnost IT by měla být standardem a kyberbezpečnost dalším nutným krokem. Mnozí zákazníci se stále obávají uložit svá data do cizího cloudu, což je naprosto legitimní. Některým ale chybí specializovaní pracovníci, anebo další prostředky na dostatečnou ochranu dat a zálohování. Proto se zajímají o tzv. hybridní model a některé z kritických služeb odebírají od technologicky vyspělých firem jako je K-net. Sdílením nejpokročilejších technologií lze omezit dopady kyberútoků a neplánovaných odstávek za ekonomicky příznivých podmínek. Nárůst zájmu o tyto služby evidujeme již nyní a dá se předpokládat jejich další masivní rozvoj.

Bezpečnost byla tématem letošního 16. Zákaznického dne. Bezpečnost je jednou z našich hlavních priorit. Proto přijměte tento malý dárek – bezpečné soukromí – krytku na webkameru.

En | *Among trends for the next year, we can see three main topics. First, a further spread of online communication. Second, an increased concern about cyber security due to a sharp increase in remote working and "popularity" of cryptovirus attacks. Third, securing a business continuity supported by IT is increasingly difficult and therefore migration to cloud or hybrid scenarios are to be on agenda.*

Jaké další trendy představuje Tomáš Knettig? Čtěte celý článek na

k.k-net.cz/trendy2021

A jaké jsou vaše vize pro rok 2021?

Podělte se s námi o své vize, napište nám je na e-mail **vize@k-net.cz**.

KDE NÁS NAJDETE?

Objednejte si Login do vaší schránky: login.k-net.cz

K-net Technical International Group, s.r.o.
Olomoucká 170
627 00 Brno – Černovice
tel.: 548 220 150
GSM: 734 686 001

Pobočka: Rovečínská 16
679 74 Olešnice
tel.: 511 447 055

K-net Team Praha, s.r.o.
Sazečská 560/8
108 00 Praha 10 – Malešice
tel.: 734 686 014

K-net Team Ostrava, s.r.o.
Smetanovo náměstí 328/1
702 00 Ostrava
tel.: 734 686 012

Facebook
facebook.k-net.cz

LinkedIn
linkedin.k-net.cz

YouTube
youtube.k-net.cz

E-mail
info@k-net.cz

www.k-net.cz

Vysvětlení podtržených výrazů z Loginu a Manažerské přílohy najdete v glosáři IT pojmů na **k.k-net.cz/glosar**.

Časopis LOGIN 2/2020, ročník č. 15 | *Připravili: Jana Hejtmánková, Blažena Kamasová, Věra Staňková, Jana Houdková, Jan Knettig, Tomáš Knettig, Petr Nepustil, Michal Štourač, Jiří Zahradník*
Malba: Jana Knettigová | Vydala společnost K-net | Neprodejné | Uzávěrka čísla: 1. 12. 2020