KYBERNETICKÁ OCHRANA JE KOMPLEXNÍ DISCIPLÍNA

strana 6

16 Sprinx

Sprinx je na trhu již od roku 1996 a po celou dobu se specializuje na CRM a obchodní systémy na míru. Cílem firmy je zákazníkovi poskytnout komplexní a vzájemně integrovaná technologická řešení, která jsou potřebná pro úspěch na poli digitální ekonomiky. Zákazníkům nabízíme tvorbu a implementaci Sprinx CRM, robustních e-shopů a portálů s nejmodernějšími marketingovými nástroji či aplikační hosting a IT outsourcing. Sprinx je také významný dodavatel IT řešení do farmaceutického průmyslu a produktů HPC (High Performance Computing).

THE DOERS
TEXT: Radek Kubeš, Jan Kotlín, Tomáš Hájek, Vít Madron, Jiří Jinger, Štefan Gorej
FOTO: Michael Kratochvíl, Václav Jedlička, archiv Sprinx, archiv FraveBot, archiv Seyfor, Shutterstock

T: 251 014 211
E: obchod@sprinx.com; pharma@sprinx.com
A: Sprinx Systems, a. s.
Údolní 212/1, 147 00 Praha 4

SPRINX **THE DOERS** SPRINX UMÍ ZABRAT A NABÍZÍ FUNKČNÍ ŘEŠENÍ. CHCE BÝT SVÝM KLIENTŮM SPOLEHLIVÝM PARTNEREM, KTERÝ RUČÍ ZA VÝSLEDEK.

DOERS
správná výslovnost:
Doer – [ˈduːər]

THE DOERS znamená, že pro Sprinx je důležitý výsledek práce. Záleží mu na spokojenosti klienta. Zná cestu od myšlenky k její realizaci.

Vážení čtenáři,

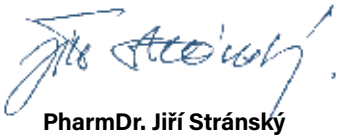
stejně jako každý rok má i ten letošní mnoho významných výročí. Některá se budou slavit hlasitě, jiná spíše potichu a některých si nezasvěcení ani nevšimnou. I já bych si dovolil jedno z výročí připomenout. Je bezesporu ze skupiny těch „pro zasvěcené" a možná ani řada z nás jej v běhu dní nezaznamená. Skutečností ale je, že v letošním roce uběhne 15 let od chvíle, kdy se změnil proces posuzování cen a úhrad léčivých přípravků v ČR. V roce 2008 byl odstartován elektronický a částečně (až plně) bezkontaktní proces, kterému podle jeho procesního postupu říkáme „správní řízení".

Bezkontaktností se míní zejména odstranění nutnosti fyzického setkávání, případně fyzického posuzování žádostí, jak bylo dříve zvykem. A díky tomu, že proces nyní probíhá plně elektronicky, je možné využít všech vymožeností digitálního světa k lepšímu a úplnějšímu posuzování přípravků, které do systému chtějí vstoupit, a k revizi stavu u těch, které tam již jsou.

Digitalizace procesu přinesla účastníkům řízení i nové možnosti, protože co je digitalizováno, může být snadno zpřístupněno, a co je zpřístupněno, může být snadno monitorováno. Účastníci řízení mohou nyní sledovat jeho průběh velmi detailně, včetně nahlížení do dokumentů, a mají možnost být upozorněni na změny v různých fázích procesu.

A jak to vše souvisí s námi? Především tak, že téměř po celou dobu existence správních řízení poskytujeme našim klientům uživatelsky příjemné nástroje na aktivní monitoring jejich průběhu. Takže toto výročí za oslavu určitě stojí.

Váš



PharmDr. Jiří Stránský
Business Director Pharma

OBSAH

FSC www.fsc.org MIX Papír | Podporujeme zodpovědné lesnictví FSC® C100605

DATUM VYDÁNÍ: 27. 6. 2023, pololetník, **MK ČR E** 23939, **MÍSTO VYDÁNÍ:** Praha
VYDAVATEL A VÝROBA: Sprinx Systems, a. s., Údolní 212/1, 147 00 Praha 4, IČ: 26770211, tiskové chyby jsou vyhrazeny.
GRAFICKÉ ZPRACOVÁNÍ: Boomerang Communication, s. r. o., Nad Kazankou 708/37, 171 00 Praha 7, www.boomerang.agency

T Marketing Sprinx **F** Shutterstock

pocketservice

NOVÁ SERVISNÍ APLIKACE Z DÍLNY SPRINXU

Ve Sprinxu jsme vyvinuli webovou aplikaci Pocketservice, určenou pro servisní techniky. Aplikace Pocketservice běží ve webovém prohlížeči a umožňuje vyplňovat servisní protokoly společně se seznamem použitých součástek a spotřebního materiálu. Díky tomu je možné okamžitě vystavit a odeslat zákazníkovi fakturu – bez ručního přepisování dat.

Pocketservice na jediném místě udržuje kompletní přehled o komunikaci se zákazníkem, dodaných produktech, poskytnutých službách, reklamacích i servisu – včetně objednávek, faktur nebo fotodokumentace. Aplikace je připravena na plánování výjezdů servisních techniků k zákazníkům a optimalizaci jejich tras, stejně jako na integraci s ERP a skladovými systémy.

CHCETE SE ZBAVIT PŘEPISOVÁNÍ A DIGITALIZOVAT PROCES POSKYTOVÁNÍ SERVISU? OZVĚTE SE NÁM A MY VÁM POSKYTNEME ZKUŠEBNÍ VERZI APLIKACE POCKETSERVICE NA 50 DNÍ ZDARMA.

50

SPRINX JE ZAKLÁDAJÍCÍM ČLENEM ASOCIACE POSKYTOVATELŮ DAT VE ZDRAVOTNICTVÍ

S myslem nově vznikající Asociace poskytovatelů dat ve zdravotnictví (APDZ) je usilovat o kultivaci právního a regulačního prostředí v oblasti ochrany, dostupnosti a zpracování dat ve zdravotnictví v České republice.

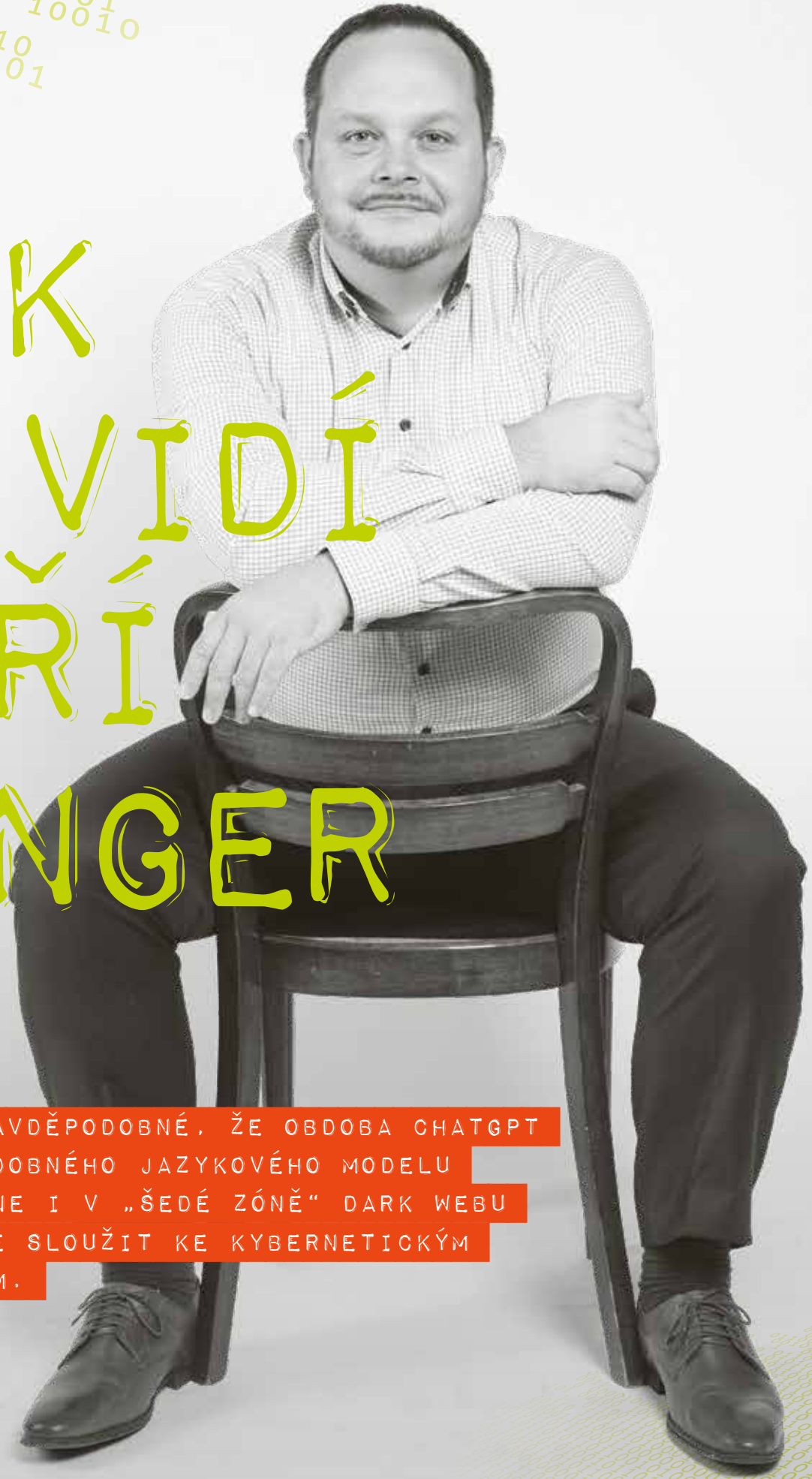
APDZ SDRUŽUJE POSKYTOVATELE A ZPRACOVATELE ZDRAVOTNICKÝCH DAT, S CÍLEM ZAJISTIT VYŠŠÍ STANDARD JEJICH SBĚRU, KONTROLY, ZPRACOVÁNÍ, ANALÝZY A PUBLIKOVÁNÍ V SOULADU S VEŘEJNÝMI ZÁJMY.

Členové asociace se zavazují vytvářet transparentní a nediskriminační prostředí a garantovat bezpečný přístup k sekundárním zdravotním datům pro jejich zpracování a efektivní využívání ve prospěch pacientů. APDZ se bude angažovat v řešení klíčových problematik v evropském zdravotnictví, které mohou zlepšit efektivitu zdravotní péče v rámci EU, s důrazem na prosazení implementace celoevropského ekosystému sběru a sdílení elektronických dat dle směrnice EHDS (European Health Data Space).

E-shop skutečně pro každého

Sprinx zaznamenal zvýšenou poptávku po implementaci e-commerce řešení, dostupnějších všem, kteří chtějí spustit nebo modernizovat svoje obchodování na internetu. Naši analytici důkladně prozkoumali a porovnali vhodná e-commerce řešení a jako nejvhodnější se rozhodli preferovat platformu Shopify. Shopify je cloudová e-commerce platforma, jejíž základní funkce lze rozšířit prostřednictvím rozsáhlé nabídky doplňkových aplikací. Díky tomu lze řešit například i napojení e-shopu na různé srovnávače cen, platební metody, dopravce a další služby. K dispozici jsou i nástroje na automatizaci a personalizaci, stejně jako napojení na ERP a skladové nebo logistické systémy. Díky kombinaci služeb a zkušeností Sprinxu s platformou Shopify mohou obchodníci získat velmi kvalitní řešení e-shopu s nízkými náklady na implementaci i provoz. Rádi vám možnosti platformy Shopify představíme společně s plánem, jak spustit moderní e-shop během několika týdnů.

JAK TO VIDÍ JIŘÍ JINGER



JE PRAVDĚPODOBNÉ, ŽE OBDOBA CHATGPT ČI PODOBNÉHO JAZYKOVÉHO MODELU VZNIKNE I V „ŠEDÉ ZÓNĚ“ DARK WEBU A BUDE SLOUŽIT KE KYBERNETICKÝM ÚTOKŮM.

SPĚJEME K SOUBOJI STROJŮ?

T Marketing Sprinx **F** archiv, Shutterstock

Snad o ničem se v oblasti IT v posledních měsících nemluví více než o technologii umělé inteligence. I když možná jedno téma má v diskusích podobnou popularitu – kybernetická bezpečnost. Jak to spolu souvisí a kde se tato dvě témata protínají? Překvapivě možná více, než by se mohlo zdát. A do budoucna se jedno bez druhého rozhodně neobejde.

AI V RUKÁCH HACKERŮ...

Jazykové modely typu ChatGPT umí vygenerovat nejen diplomovou práci v prakticky jakémkoli oboru, ale poradí si i s vytvářením skriptů a celých programů. Omezení daná tvůrci těchto modelů brání AI splnit úkol typu „Naprogramuj mi nezjistitelný virus", ale lze je celkem snadno obejít. Například můžete umělé inteligenci zadat roli vývojáře a pověřit ji analýzou kódu s cílem odhalení jeho slabin. To pak může vést třeba k útokům na společnosti využívající různá open source řešení.

V budoucnu navíc můžeme očekávat, že se jazykové modely typu ChatGPT zapojí také na „temné" straně, pod kterou si můžeme představit třeba Dark web. Dnes jsou zde dostupné například nástroje na provádění phishingových a ransomwarových útoků a se stále větší dostupností obrovského výpočetního výkonu zde může vzniknout AI pro hackery, která žádné „etické brzdy" mít nebude.

... I OBRÁNCŮ

V kyberbezpečnosti není využití AI žádnou novinkou. Už dnes nám pomáhá například s analýzou síťového provozu a odhalováním anomálií, které mohou být indikátorem probíhajícího útoku. Nasazení AI v bezpečnostních řešeních bude do budoucna určitě mnohem intenzivnější, protože znalostní báze a kapacita výkonu pomůže ještě rychleji analyzovat mnohem větší množství dat posbíraných ze zařízení po celém světě – a tedy i mnohem rychleji reagovat na nové hrozby. AI se posune i do koncových zařízení, kde pomůže například s odhalováním phishingu.

VŽDY ZÁLEŽÍ NA LIDECH

Souboj strojů, které na jedné straně vymýšlejí nové typy útoků a na druhé zase obranu proti nim, by se točil v kruhu – kdyby nebylo lidí. Tak jako při analýze snímků a laboratorních výsledků sice může velmi pomoci umělá inteligence, ale konečné stanovení diagnózy a způsobu léčby je už na zkušených lékařích, budou i v kyberbezpečnosti (alespoň) zatím hrát zásadní roli schopnosti lidských expertů. Ti rozhodnou, jak se na útoky připravit a jak minimalizovat následky úspěšného napadení. A je také na lidech, aby umělé inteligenci stanovili mantinely. Nikoli v tom, co by měla umět a dělat, ale je třeba určit, jak hluboko ji do své organizace pustíme a jaké informace budeme s jazykovými modely sdílet. Před takovým rozhodnutím už možná stojíme právě teď.

TIP

PODLE STUDIE FORTINET 2023 GLOBAL RANSOMWARE REPORT JSOU HLAVNÍMI TAKTIKAMI ÚTOČNÍKŮ PŘI INFILTRACI RANSOMWARU DO SÍTĚ PHISHING, VYUŽITÍ PORTŮ OTEVŘENÝCH DO INTERNETU A ZNEUŽITÍ PROTOKOLU VZDÁLENÉ PLOCHY.

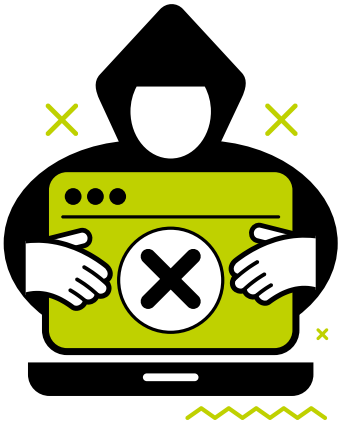
JIŘÍ JINGER

Ve Sprinxu pracuje Jiří Jinger už více než 10 let, v současnosti na pozici manažera pro kybernetickou bezpečnost a cloudové služby poskytované v rámci platformy AppOn.cloud. Cloudovým službám se z hlediska jejich dostupnosti, spolehlivosti a bezpečnosti věnuje většinu své profesní dráhy. Pokud zrovna nepřemýšlí o obraně proti nejnovějším typům kyberútoků, věnuje se rád turistice, muzice (klávesy a bicí), zvelebování domu a jeho okolí, ale díky dvěma úžasným dětem je na to o poznání méně času než dříve.

T Marketing Sprinx **F** archiv, Shutterstock

5 NEJČASTĚJŠÍCH TYPŮ KYBERNETICKÝCH ÚTOKŮ **A JAK SE JIM BRÁNIT**

KYBERNETICKÁ BEZPEČNOST BY MĚLA PATŘIT K ABSOLUTNÍM PRIORITÁM KAŽDÉ FIRMY ČI ORGANIZACE. HROZBY JSOU STÁLE SLOŽITĚJŠÍ A OBRANA PŘED NIMI NÁROČNĚJŠÍ. JAKÉ JSOU NEZBYTNÉ KROKY OBRANY PROTI TĚM NEJČASTĚJŠÍM?



Průzkumy a statistiky společností z oblasti kybernetické bezpečnosti se v konkrétních údajích různí, ale v jednom se absolutně shodují – množství kybernetických útoků roste a jejich sofistikovanost se zvyšuje. Kromě vysoce cílených útoků, vedených často i státem podporovanými hackerskými skupinami za účelem špionáže nebo poškození cílených subjektů, jsou nebezpečné především ransomwarové útoky, vedené s cílem získat peníze na výkupném za dešifrování dat, stejně jako phishingové útoky, které mají oklamat svůj cíl a přimět jej udělat nějakou akci (vyzradit citlivé informace, zaplatit falešnou fakturu atd.). Množí se ale také plošné, v zásadě amatérskými útočníky vedené phishingové a ransomwarové kampaně, které lze relativně snadno provádět s nástroji typu ransomware-as-a-service a phishing-as-a-service. Takové útoky lze sice snadněji odhalit a zastavit, ale při minimálních nákladech a širokém dosahu se útočníkům vyplatí i při velmi nízké úspěšnosti.

Celkově existuje dlouhá řada různých typů kybernetických útoků, ale zkušenosti ukazují, že podnikům hrozí především pět způsobů útoků, které si následně popíšeme, stejně jako klíčové kroky obrany proti nim. Zcela běžné jsou přitom kombinace vektorů útoků, které například často začínají phishingem s cílem získat přístup do sítě, pokračují průzkumem napadeného cíle a odcizením cenných dat a vyvrcholí nasazením ransomwaru. Také proto neexistuje jediné univerzální řešení kyberbezpečnosti, ale účinná obrana se vždy skládá hned z několika prvků.

V PRVNÍ POLOVINĚ ROKU 2022 ZAZNAMENALI SPECIALISTÉ FORTIGUARD LABS 10 666 NOVÝCH VARIANT RANSOMWARU, COŽ JE DVOJNÁSOBEK POČTU ZJIŠTĚNÉHO V PŘEDCHOZÍCH ŠESTI MĚSÍCÍCH.

1 NENECHTE SE NACHYTAT NA PHISHING

Phishing je technika, při níž útočníci zasílají falšované e-maily, které vypadají jako od důvěryhodných zdrojů, aby přiměli oběti k poskytnutí citlivých informací. Typicky jde o přihlašovací údaje, hesla nebo různé finanční informace. Extrémně nebezpečný je tzv. spear-phishing, tedy pečlivě připravený podvrh na konkrétní osobu ve firmě, která má například pravomoc provádět platby dle zaslaných instrukcí.

Na rozdíl od prvotních pokusů před několika lety jsou dnešní phishingové e-maily často perfektně připravené – s dokonalou češtinou i grafickou úpravou a odkazy na důvěryhodně vypadajících doménách. Rozpoznání phishingu je proto stále složitější a extrémně důležitou roli hraje ostražitost uživatele, kterému podvržená zpráva přijde do schránky. Jak se bránit?

Vzdělávejte všechny zaměstnance: Ujistěte se, že rozumíte tomu, co je phishing a jaké jsou jeho různé formy. Učte se rozpoznávat podezřelé e-maily, odkazy a webové stránky.

Pečlivě kontrolujte e-maily: Důkladně kontrolujte e-maily od neznámých odesílatelů nebo zprávy, které vypadají podezřele. Podívejte se na e-mailovou adresu odesílatele a zkontrolujte, zda je to skutečná adresa společnosti nebo osoby, kterou znáte.

Nevkládejte citlivé informace do neověřených formulářů: Nikdy nezadávejte hesla, finanční informace nebo osobní údaje do formulářů, které nebyly ověřeny. Zkontrolujte adresu webové stránky a ověřte si, že používá šifrovaný protokol https.

Neotevírejte podezřelé přílohy: Přílohy e-mailů mohou obsahovat škodlivý software nebo odkazy na škodlivé webové stránky. Pokud si nejste jistí pravostí e-mailu, neotevírejte přílohy ani neklikejte na odkazy.

Používejte dvoufaktorové ověřování a silná hesla: I když útočník získá vaše heslo, stále bude potřebovat druhý faktor (například textovou zprávu nebo aplikaci pro generování kódů) pro přístup k vašemu účtu.

2 VÝKUPNÉ ZA VAŠE DATA

Ransomware je druh škodlivého softwaru, který zašifruje data v napadeném systému a požaduje výkupné za jejich obnovení (které ale není jisté ani v případě zaplacení). Útočníci často žádají o platbu v kryptoměnách, aby byli těžko vystopovatelní. Jeden z nejznámějších ransomwarových útoků proběhl v roce 2019 v benešovské nemocnici. Ta přišla například o internetový objednávkový systém pro dárce krve, stejně jako o část administrativních a ekonomických dat. Kyberútok způsobil škodu za asi 59 milionů a pachatele se vypátrat nepodařilo. Obrana vyžaduje několik opatření:

Zálohujte svá data: Díky pravidelným zálohám důležitých dat na externím úložišti nebo v cloudu bude v případě ransomwarového útoku možné obnovit data ze záloh.

Aktualizujte software: Udržujte svůj operační systém, prohlížeč a všechny aplikace aktuální. Aktualizace často obsahují opravy zranitelností, které mohou být zneužity ransomwarem.

Používejte antivirový software: Instalujte a pravidelně aktualizujte kvalitní antivirový software, který dokáže detekovat a blokovat ransomware.

Buďte opatrní při otevírání e-mailových příloh a klikání na odkazy: Ransomware může být doručen prostřednictvím phishingových e-mailů, které obsahují škodlivé přílohy nebo odkazy.

Zkontrolujte oprávnění: Omezte oprávnění uživatelů ve vašem systému tak, aby neměli přístup k více souborům, než je nezbytně nutné. To může pomoci omezit rozsah škod.

KOLIK STOJÍ RANSOMWAROVÝ ÚTOK?

Pokud jim to neukládají předpisy, firmy a organizace se úspěšným napadením své sítě zpravidla nechlubí, stejně jako nezveřejňují výši nákladů na řešení obnovy dat nebo zaplacení výkupného. Existuje ale řada průzkumů popisujících průběh a následky (nejen) ransomwarových útoků. Například aktuální studie The State of Ransomware 2023 od společnosti Sophos, která vychází z průzkumu mezi 3 000 firem a organizací ve 14 zemích světa, uvádí:

66 %
organizací zaznamenalo v uplynulém roce ransomwarový útok (nejčastější příčinou byly zranitelnosti softwaru a odcizené přihlašovací údaje).

76 %
útoků skončilo zašifrováním dat (ve 30 % útočníci data nejprve odcizili).

97 %
organizací získalo svá data zpět (46 % obětí zaplatilo výkupné).

1 540 000 $
je střední hodnota požadovaného výkupného.

84 %
obětí ransomwaru utrpělo i ztráty na obratu.

24 %
napadených organizací potřebovalo ke zotavení po útoku 1 až 6 měsíců.

Bez započítání zaplaceného výkupného je střední hodnota nákladů na obnovu po ransomwarovém útoku
1 820 000 $
(1,6 milionu dolarů při obnově dat za zálohy a 2,6 milionu při zaplacení výkupného).

JIŘÍ JINGER

3 POD ÚTOKEM ZE VŠECH STRAN

Útoky typu DDoS (Distributed Denial of Service) představují zahlcení webových serverů nebo sítí velkým množstvím falešného provozu, což vede k přetížení systému a jeho nedostupnosti pro legitimní uživatele. Obrana je složitá, ale dopad útoků lze přinejmenším zmírnit:

Nasaďte síťová bezpečnostní zařízení: Firewally a systémy prevence intruzí (IPS) filtrují síťový provoz a detekují podezřelé vzory, které mohou naznačovat DDoS útok. Zablokují falešný provoz a propustí legitimní požadavky.

Implementujte Web Application Firewall: WAF dokáže filtrovat a monitorovat HTTP provoz mezi internetem a vaší webovou aplikací a může pomoci identifikovat a blokovat škodlivý provoz.

Používejte cloudové služby nebo služby na ochranu před DDoS: Díky značné šířce pásma a rozsáhlým zdrojům mohou cloudové služby snadněji absorbovat DDoS útoky. Cloudové služby mohou také poskytnout záložní servery, pokud je váš hlavní server napaden. Specializované služby, jako jsou Cloudflare, Akamai nebo Amazon Web Services Shield, mají schopnost rozpoznat a blokovat DDoS útoky v reálném čase.

Zajistěte ochranu DNS serveru: Ujistěte se, že váš DNS server je chráněn před DDoS útoky tím, že používáte redundanci, geografickou distribuci a kešování.

ESET THREAT REPORT T3 2022 UVÁDÍ: I PŘES POKLES POČTU RDP ÚTOKŮ BYLO V POSLEDNÍ TŘETINĚ ROKU 2022 STÁLE NEJOBLÍBENĚJŠÍM VEKTOREM SÍŤOVÝCH ÚTOKŮ HÁDÁNÍ HESEL. NA DRUHÉM MÍSTĚ V ŽEBŘÍČKU ÚTOKŮ ZVENČÍ SE UMÍSTILY ÚTOKY ZNEUŽÍVAJÍCÍ ZRANITELNOST LOG4J – PŘESTOŽE JE PRO NI K DISPOZICI OPRAVA JIŽ OD PROSINCE 2021.

PŘIPRAVTE SE NA RIZIKA

Základem odolnosti proti kybernetickým rizikům je příprava, například implementací ISMS (Information Security Management System). Systém řízení informační bezpečnosti je soubor politik, postupů, procesů a kontrolních mechanismů, které organizace zavede a použije k řízení, monitorování a zlepšování informační bezpečnosti. Cílem ISMS je chránit důvěrnost, integritu a dostupnost informací a systémů v organizaci. ISMS většinou zahrnuje tyto složky:

Bezpečnostní politika: Definuje základní principy, cíle a směrnice, které organizace používá k řízení informační bezpečnosti.

Řízení rizik: Proces identifikace, hodnocení a řízení rizik spojených s informační bezpečností.

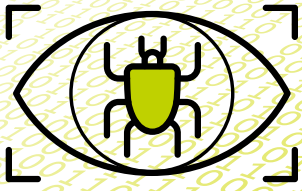
Kontrolní mechanismy: Soubor technických, fyzických a organizačních opatření, která organizace implementuje k ochraně informačních aktiv a minimalizaci rizik.

Incident management: Proces identifikace, řešení a analýzy bezpečnostních incidentů a narušení informační bezpečnosti.

Monitoring a revize: Pravidelné sledování, hodnocení a revize bezpečnostních politik, postupů, kontrol a rizik, aby se zajistilo, že ISMS zůstává účinný a aktuální.

Kontinuální zlepšování: Proces zlepšování informační bezpečnosti a ISMS na základě zjištění z revizí, hodnocení rizik a analýzy incidentů.

ISMS se následně zastřešuje například certifikací ISO 27001, která má organizacím pomoci zavést a udržovat efektivní rámec pro identifikaci, hodnocení a řízení rizik spojených s informační bezpečností.



4 VZPOURA TISKÁREN A TERMOSTATŮ

Také nezabezpečená zařízení internetu věcí (IoT), jako jsou chytré televizory, kamery, síťové tiskárny nebo třeba termostaty, mohou být zneužita útočníky k vytvoření sítě botnetů a provádění DDoS útoků. Jakékoli zařízení připojené k síti musí být zabezpečeno:

Aktualizujte firmware a software: Pravidelně aktualizujte firmware a software vašich IoT zařízení, aby byla chráněna před známými zranitelnostmi.

Změňte výchozí hesla: Mnoho IoT zařízení je dodáváno s výchozími hesly, která jsou snadno dostupná útočníkům. Změňte je na silná a jedinečná hesla pro každé zařízení.

Oddělte IoT zařízení od hlavní sítě a monitorujte jejich provoz: Vytvořte oddělenou síť (VLAN) pro IoT zařízení, aby byla izolována od vaší hlavní sítě. Minimalizujete tak riziko, že útočník získá přístup k citlivým informacím prostřednictvím nezabezpečených IoT zařízení.

Omezte přístup k IoT zařízením i jejich množství: Nastavte přístup k IoT zařízením pouze pro oprávněné uživatele a zvažte, zdali jsou všechna zařízení nezbytná.

Instalujte bezpečnostní opatření na úrovni sítě: Použijte firewally, systémy detekce a prevence průniku (IDS/IPS) a další síťová bezpečnostní zařízení, která mohou identifikovat a blokovat útoky na IoT zařízení.

5 ROKY NEOŠETŘENÉ ZRANITELNOSTI

Velmi častým prostředkem úspěšných útoků jsou neošetřené zranitelnosti softwaru, jako chyby v kódu nebo špatné konfigurace. Alarmující je množství útoků realizovaných prostřednictvím zranitelností, na které již dlouhou dobu existují záplaty. Vyhněte se těmto rizikům:

Používejte ověřený a důvěryhodný software od renomovaných výrobců: Vyhněte se použití nelegálního nebo neautorizovaného softwaru, který může obsahovat skryté zranitelnosti nebo malware.
Pravidelně aktualizujte veškerý software: operační systém, aplikace, frameworky i jakýkoli další software.

Provádějte pravidelné skenování zranitelností: Používejte nástroje na skenování zranitelností, které vám pomohou identifikovat slabá místa v softwaru a systémech a opravit je dříve, než je mohou útočníci zneužít.

Zkontrolujte konfiguraci: Ujistěte se, že váš software je správně nakonfigurován a zabezpečen. Špatně nakonfigurovaný software může obsahovat zneužitelné zranitelnosti.

Kontrolujte oprávnění a přístup: Omezte přístup k systémům a softwaru na nezbytné úrovně. Ujistěte se, že přístup k citlivým informacím a zdrojům mají pouze oprávnění uživatelé.

Náš výčet kybernetických rizik a souvisejících opatření samozřejmě nemůže být konečný. Specialisté Sprinxu mají bohaté zkušenosti jak se zabezpečením našich vlastních cloudových služeb, tak s řešením bezpečnosti u našich zákazníků. Spojte se s námi, abychom společně prověřili vaše kybernetické zabezpečení a navrhli jeho posílení tam, kde je potřeba.

TIP

KYBERNETICKÁ BEZPEČNOST ZAČÍNÁ A KONČÍ U LIDÍ – PŘEDSTAVUJÍ PRVNÍ LINII OBRANY A ČASTO SVÝM ROZHODNUTÍM MOHOU ÚTOK ZASTAVIT, NEBO PUSTIT DO SÍTĚ. PAMATUJTE NA TO PŘI VZDĚLÁVÁNÍ ZAMĚSTNANCŮ.

T redakce **F** archiv Seyfor

TIP

Z HLEDISKA KYBERBEZPEČNOSTI BUDE CLOUDOVÁ SLUŽBA, O KTEROU SE STARÁ TÝM ZKUŠENÝCH SPECIALISTŮ, ODOLNĚJŠÍ NEŽ PODNIKOVÉ SERVERY.

ZÁLEŽÍ NÁM PŘEDEVŠÍM NA SPOLEHLIVOSTI A STABILITĚ

SPOLEČNOST SEYFOR VZNIKLA V ROCE 1990 POD NÁZVEM CÍGLER SOFTWARE A V ROCE 2014 SE PO NĚKOLIKA AKVIZICÍCH PŘEJMENOVALA NA SOLITEA. DALŠÍ VLNA AKVIZIC, SPOLEČNĚ S PRONIKÁNÍM NA NOVÉ TRHY V ZÁPADNÍ EVROPĚ ČI NA BALKÁNĚ, PŘINESLA KONCEM ROKU 2022 I ZMĚNU NÁZVU NA SEYFOR.

Dnes je Seyfor jedním z nejvýznamnějších dodavatelů ERP a dalších podnikových systémů ve střední Evropě, s více než třemi desítkami různých programů a aplikací, 1 600 zaměstnanci v rámci celé skupiny a zákazníky ve 38 zemích světa. V roce 2022 dosáhla skupina Seyfor tržeb ve výši 2,97 miliardy korun.

Skoro od samého počátku je s firmou i Tomáš Komárek, který prošel od pozice testera přes konzultanta a projektového manažera až ke své dnešní pozici ředitele ekonomického systému Money ERP. A prakticky stejnou dobu spolupracuje s předním dodavatelem ERP systémů, s vlajkovým produktem Money, také Sprinx Systems.

Jak vaši klienti dnes vnímají cloud, je ještě nutné je přesvědčovat o jeho výhodách?

Naši zákazníci vnímají cloud jako jasnou alternativu k provozu podnikových aplikací vlastními silami – dnes už prakticky bez obav z hlediska ochrany dat nebo spolehlivosti a dostupnosti systémů. To ale neznamená, že si rádi neposlechnou také o dalších výhodách cloudu, jako je mobilita nebo flexibilita nákladů, tedy možnost rychlého spuštění aplikací bez velkých počátečních investičních nákladů a také řízení provozních nákladů podle skutečného využití a počtu uživatelů. To mimochodem znamená, že jsou dnes vyspělé podnikové aplikace dostupnější i start-upům a menším firmám, které prostě příliš investovat nemohou.

APPON.CLOUD JE PRO NÁS SPOLEHLIVÉ PROSTŘEDÍ, KTERÉ SE DYNAMICKY PŘIZPŮSOBUJE AKTUÁLNÍM POTŘEBÁM APLIKACÍ A ZA VŠECH OKOLNOSTÍ ZAJIŠŤUJE JEJICH VYSOKOU DOSTUPNOST NAŠIM ZÁKAZNÍKŮM.

Znamená to tedy, že cloud je primárně finanční volbou?

Když pomineme všechny ostatní výhody, tak si firmy určitě umí dobře spočítat, kolik musí investovat do nového hardwaru, aby mohly provozovat vždy aktuální verzi ERP systému, stejně jako třeba do nezbytných licencí. Celý trh totiž hlavní dodavatelé podnikového softwaru směřují k tomu, že si klasické licence serverových systémů nebo databází pořizují skutečně jen firmy, které je opravdu potřebují. Ostatní vsadí spíše na nějakou formu hostingu nebo rovnou na cloud, kde je o hardware i software postaráno. Zvlášť pokud si připočtou i další náklady na zabezpečení, zálohování nebo nepřetržitý monitoring. Provoz aplikací prostě není vůbec snadná ani levná záležitost, což je i jeden z důvodů, proč spolupracujeme právě se Sprinxem.

Je provoz aplikací v cloudu výhodou i z hlediska kyberbezpečnosti?

Z naší zkušenosti rozhodně ano. Pokud máte opravdu kvalitního a zkušeného

Tomáš Komárek, ředitel Business Unit Money ERP ve společnosti Seyfor, a. s.

30
SEYFOR DODÁVÁ VÍCE NEŽ TŘI DESÍTKY RŮZNÝCH PROGRAMŮ A APLIKACÍ

1600
ZAMĚSTNANCŮ V RÁMCI CELÉ SKUPINY

38
PŮSOBÍ VE 38 ZEMÍCH SVĚTA

2,97 mld. Kč
TRŽBY DOSAŽENÉ V ROCE 2022

poskytovatele cloudových služeb, budou aplikace provozované v cloudu proti kyberútokům odolnější oproti systémům provozovaným na vlastních serverech. Víme například hned o několika našich zákaznících, kteří se po ransomwarovém útoku museli vyplatit v bitcoinech, aby získali zpět svá zašifrovaná data v ERP, provozovaném na vlastních serverech. Oproti tomu u platformy AppOn.cloud jsme zatím žádný závažný bezpečnostní incident nezaznamenali. Přestože samozřejmě víme, že kybernetické útoky se cloudovým službám nevyhýbají.

Ale nejde jen o kyberútoky, důležitá je i fyzická bezpečnost. Máme zákazníky, kterým voda zničila nejen sklad plný zboží, ale také servery s ERP a všemi daty. Rizika bych mohl vyjmenovávat dlouho, takže je opravdu rozumné svěřit kriticky důležité aplikace a data spolehlivému poskytovateli cloudových služeb, který musí být na všechny možnosti ohrožení připravený.

Pamatujete si ještě na začátky spolupráce se Sprinxem? Čím vás přesvědčil?
Ve firmě už budu dvacet let a spolupráce se Sprinxem začala ještě předtím. Už to o něčem svědčí, a také proto jsme se nedávno rozhodli naši spolupráci ještě prohloubit. Výsledkem je, že dnes je pro nás Sprinx a jeho platforma AppOn.cloud preferovaným poskytovatelem aplikačního hostingu v cloudu. To znamená, že pokud si naši zákazníci přejí provozovat naše systémy Money v cloudu, doporučíme jim právě Sprinx a AppOn.cloud.

Sprinx tedy preferujete i před globálními poskytovateli cloudových služeb?
Určitě ano, už proto, že jde o stabilního, lokálního partnera, se kterým máme dlouholetý vztah a který velmi dobře rozumí našim produktům. To je pro nás obrovsky důležité, protože díky tomu můžeme daleko rychleji reagovat na jakýkoli problém a nemusíme pokaždé nejprve řešit, kdo je za co zodpovědný a kdo má co vyřešit. Technici Sprinxu, kteří se o aplikace běžící na AppOn.cloud starají, zpravidla problémy vyřeší, aniž by bylo nutné je eskalovat k nám. To nám velmi šetří práci a zvyšuje spokojenost zákazníků, protože jsou jejich požadavky na technickou podporu vyřešeny velmi rychle. Navíc se velmi snadno domluvíme, co přesně provoz našich aplikací vyžaduje, a Sprinx nám to v AppOn.cloud připraví.

Plánujete spolupráci se Sprinxem dále rozšířit?
Ještě nemohu odtajnit detaily, ale společně se Sprinxem uvažujeme o možnosti, jak ještě více zpřístupnit vyspělé ERP a ekonomické řešení menším podnikům a start-upům – s kompletními možnostmi, ale s minimální vstupní investicí. Aktuálně na nové možnosti využívání našich produktů v cloudu pracujeme a už brzy odhalíme víc. ●

Seyfor

B2B E-SHOP

PRO DODAVATELE PRACOVNÍCH ODĚVŮ A OCHRANNÝCH POMŮCEK

SPRINX CONSULTING SPRÁVNĚ VYSTIHL POTŘEBU KLIENTA, KTERÝ ZÍSKAL MODERNÍ E-COMMERCE ŘEŠENÍ S PRVKY AUTOMATIZACE A INTEGRACÍ NA ERP SYSTÉM.

T Radek Kubeš **F** Shutterstock

Firma Blyth, s.r.o., založená v roce 1992 jako dceřiná společnost britského partnera W. A. Blyth Ltd., je od roku 2016 součástí globálního koncernu Bunzl se 170letou tradicí. Blyth poskytuje kompletní nabídku osobních ochranných pracovních prostředků (OOPP) od všech významných světových výrobců. Na základě poradenství a auditů v oblasti prevence a ochrany zdraví zaměstnanců odebírají zákazníci společnosti Blyth pracovní oděvy a obuv, rukavice i řadu dalších typů ochranných pomůcek. Mezi zákazníky společnosti Blyth patří největší výrobci v automobilovém průmyslu i firmy z oboru stavebnictví, gastronomie a mnoha dalších oblastí.

B2B OBCHODOVÁNÍ MÁ SVÁ SPECIFIKA

Společnost Blyth se na Sprinx Consulting obrátila s požadavkem na inovaci svého stávajícího e-shopu, který již nevyhovoval současným požadavkům na digitální obchodování mezi podniky. Blyth na svém webu nabízel katalog produktů a funkce pro nakupování způsobem vhodným především pro koncové zákazníky, kteří ale nejsou cílovou skupinou velkoobchodníka s pracovními oděvy a ochrannými pomůckami. Současně se prodejce potýkal i s technickými problémy, kdy se objednávky z e-shopu často nepřenášely do ERP systému, a proto nebyly vyřízeny včas.

První výzvou pro Sprinx Consulting proto bylo důkladné porozumění obchodnímu modelu společnosti Blyth a současně i procesům, na základě kterých jeho zákazníci objednávají dodávky OOPP z nabídky až desítek tisíc produktů.

Výsledkem analýzy a konzultací byla výrazná změna zadání celého projektu. Na základě doporučení konzultantů ze Sprinx Consulting se společnost Blyth rozhodla pro nasazení výhradně B2B e-commerce řešení – ovšem s komfortními a automatizačními funkcemi, na které jsme dnes zvyklí z nejlepších e-shopů pro koncové zákazníky. Přesně takové možnosti poskytuje platforma Sprinx B2B Ready, se kterou Sprinx Consulting zvítězil ve výběrovém řízení na nové e-commerce řešení společnosti Blyth.

INTEGRACE S ERP I SYSTÉMY ZÁKAZNÍKA

Sprinx B2B Ready je e-commerce platforma připravená k rychlému

TIP

„FIREMNÍ ZÁKAZNÍCI SI ZASLOUŽÍ PŘINEJMENŠÍM STEJNÝ KOMFORT NAKUPOVÁNÍ, JAKO POSKYTUJÍ SVÝM ZÁKAZNÍKŮM NEJLEPŠÍ E-SHOPY. INTEGRACE PODNIKOVÝCH SYSTÉMŮ NAVÍC UMOŽŇUJE MNOHEM VĚTŠÍ ÚROVEŇ AUTOMATIZACE.“

Blyth poskytuje kompletní nabídku osobních ochranných pracovních prostředků.

spuštění online prodeje. Je možné ji integrovat s ERP systémy pro automatické přenášení objednávek z e-shopu, šetří administrativní náklady, zrychlí prodej, sníží chybovost při zpracování objednávek a umožní automatizaci souvisejících procesů v obchodě i logistice. Právě tyto vlastnosti oceňují velkoobchodní prodejci, kteří mohou svým podnikovým zákazníkům poskytnout pohodlný způsob online objednávání zboží, respektující jejich individuální nákupní a schvalovací procesy.

ODPOVĚDÍ JE B2B READY

Sprinx nasadil platformu B2B Ready jako základ webového katalogu společnosti Blyth a ve spolupráci s dodavatelem ERP systému ABRA zajistil jeho napojení na databázi produktů i automatizované předávání objednávek zákazníků do procesu jejich zpracování.

Konzultanti Sprinxu navštívili společně s obchodními zástupci společnosti Blyth řadu největších zákazníků, aby dokonale pochopili jejich konkrétní procesy při objednávání a schvalování nákupů pracovních oděvů a ochranných pomůcek. Výsledkem je maximálně vstřícná možnost automatizovaného zadávání a schvalování objednávek, která výrazně zrychluje obchodování a zajišťuje, že budou mít zákazníci společnosti Blyth vždy k dispozici všechny potřebné produkty.

Nový B2B e-shop společnosti Blyth je provozován na cloudové platformě AppOn.cloud, která je plně pod kontrolou Sprinxu a zajišťuje spolehlivý provoz s minimální dobou odezvy. Sprinx poskytuje nepřetržitou podporu a současně řešení Sprinx B2B Ready dále rozvíjí.

Zákazníci společnosti Blyth zaznamenali s novým webovým katalogem zásadní zlepšení jeho odezvy a přehlednosti, stejně jako zvýšení komfortu objednávání. To nyní navíc zcela respektuje jejich interní procesy. V rámci další spolupráce se Sprinx Consulting připravuje společnost Blyth i možnost automatizovaného objednávání produktů přímo ze skladových systémů zákazníků, stejně jako nové možnosti individuálního přizpůsobení objednávaného zboží. ●

BUNZL BLYTH WORKWEAR

KOMFORTNÍ NAKUPOVÁNÍ

Platforma Sprinx B2B Ready umožňuje, že mohou registrovaní zákazníci společnosti Blyth objednávat pracovní oděvy, ochranné pomůcky i další zboží komfortně a s vysokou úrovní automatizace:

- V administraci zákaznického účtu lze nastavit a spravovat vlastní schvalovací proces (osoby oprávněné objednávat, finanční limity, povolené typy produktů apod.).
- Zákazníci mají k dispozici vlastní katalogy zboží společně s individuálními ceníky a platebními podmínkami.
- Objednávky lze zadávat hromadně na základě produktových čísel a importu seznamů produktů v různých formátech.
- K dispozici jsou funkce opakovaných objednávek i nákupních seznamů.
- V rámci online objednávek lze ihned zvolit individuální úpravy dle zadaných vzorů (vyšití loga, potisk atd.).

MODERNÍ E-SHOP HNED A ZA DOSTUPNOU CENU? ŽÁDNÝ PROBLÉM!

T Vít Madron **F** Václav Jedlička

NE KAŽDÝ OBCHODNÍK POTŘEBUJE ROBUSTNÍ, NA MÍRU POSTAVENÝ E-SHOP. VE SPRINXU SI TO UVĚDOMUJEME A POMŮŽEME VÁM ZAČÍT OBCHODOVAT RYCHLE A BEZ VELKÝCH INVESTIC.

TIP

ZAČNĚTE V MALÉM, ALE O TO RYCHLEJI – NA ROBUSTNĚJŠÍ, NA MÍRU VYVINUTÉ E-COMMERCE ŘEŠENÍ MŮŽETE PŘEJÍT KDYKOLI, ALE SE SPRINXEM A SHOPIFY MŮŽETE ZAČÍT OBCHODOVAT HNED.

Obchodníkům a výrobcům bez vlastního e-shopu chybí důležitý prodejní kanál, prostřednictvím kterého lze rychle a relativně levně oslovit široký okruh zákazníků. Aktuální ekonomická situace ale firmy nutí spíše snižovat náklady, než aby podporovala investice do vývoje robustního e-commerce řešení. I proto v současnosti roste poptávka po e-shopech postavených na standardizovaných cloudových platformách.

Abychom ve Sprinxu byli schopní poskytnout své zkušenosti a schopnosti i menším internetovým obchodníkům, kteří hledají levnější, předpřipravenou e-shopovou platformu, naši analytici prozkoumali a důkladně porovnali vhodná e-commerce řešení. A jako nejvhodnější jsme se rozhodli preferovat platformu Shopify.

Shopify je cloudové e-commerce řešení plně podporující českou legislativu spojenou s obchodováním na internetu. Jeho základní funkce lze zásadně rozšířit prostřednictvím skutečně rozsáhlé nabídky doplňkových aplikací. Díky tomu lze řešit například i napojení e-shopu provozovaného na Shopify na různé srovnávače cen, platební metody, dopravce a další služby. Navíc jsou k dispozici i nástroje na automatizaci a personalizaci, stejně jako napojení na ERP, skladové nebo logistické systémy.

VÍT MADRON

SHOPIFY SE SLUŽBAMI SPRINXU

Shopify je sice velmi dostupné, ale současně i poměrně rozsáhlé řešení, jehož správná implementace a napojení na zdroje dat o produktech či podnikové systémy vyžaduje specifické znalosti. Proto naši konzultanti a specialisté zajišťují obchodníkům kompletní implementaci jejich nového e-shopu na platformě Shopify, včetně všech potřebných integrací na zdroje dat a další systémy.

Sprinx může zároveň k Shopify vyvinout i specifické doplňky, které tuto obchodní platformu přiblíží individuálnímu e-commerce řešení – při nižších nákladech a s kratší dobou implementace. ●

PROČ SHOPIFY?

Díky kombinaci služeb a zkušeností Sprinxu s přední globální e-commerce platformou Shopify mohou obchodníci získat velmi kvalitní řešení e-shopu s nízkými náklady na implementaci i následný provoz a možností budoucího rozvoje.

shopify

TOMÁŠ HÁJEK:

DIGITALIZACI SI ZASLOUŽÍ KAŽDÝ

T Radek Kubeš **F** Michael Kratochvíl

ZA TÉMĚŘ PĚT LET VE SPRINXU PŘEŠEL TOMÁŠ HÁJEK OD VEDENÍ TÝMU PROJEKTOVÝCH MANAŽERŮ DO POZICE, KDY JE ODPOVĚDNÝ ZA VÝVOJ A OBCHODNÍ ÚSPĚCH VÝZNAMNÉHO PRODUKTU – NOVÉ SERVISNÍ APLIKACE. TENTO PRODUKT VYVÍJENÝ VE SPRINXU ZCELA OD ZÁKLADU JE URČEN PRO FIRMY POSKYTUJÍCÍ SLUŽBY ZÁRUČNÍHO I POZÁRUČNÍHO SERVISU V TERÉNU A PŘÍMO U ZÁKAZNÍKŮ.

Do webové aplikace usnadňující plánování i další administrativu kolem servisních zásahů brzy přibydou i funkce podporované umělou inteligencí. Zajímá vás, v čem bude AI v naší servisní aplikaci užitečná?

1 Co bylo impulzem k vývoji servisní aplikace?

Samotná myšlenka o vytvoření aplikace na digitalizaci procesů kolem poskytování servisních služeb je s námi už dlouho. Ale až konkrétní požadavek jednoho z našich zákazníků spustil proces, na jehož konci je zcela nový produkt s jasným plánem dalšího rozvoje. Jen pro zajímavost – vývoj do první provozuschopné ukázky nám trval asi dva měsíce a celou servisní aplikaci, kterou jako produkt uvedeme na začátku července, jsme vyvíjeli přibližně jeden rok.

2 Co všechno dnes servisní aplikace umí?

Soustředili jsme se především na plánování servisních zakázek (incidentních i pravidelných), udržování historie servisovaných zařízení se všemi činnostmi, komunikací i dokumentací a vytváření servisních protokolů. To je mimochodem asi jedna z nejvíce „digitálních" funkcí, která obrovsky šetří čas, odstraňuje chyby při přepisování papírových formulářů a zrychluje proplacení servisních zakázek. Aplikace umí pracovat také se skladovými zásobami, hlasové poznámky přepisuje na text a je dostupná ve 4 jazycích.

3 Pro jaké zákazníky je servisní aplikace určena?

Naše aplikace pomůže s digitalizací především poskytovatelům servisu a údržby gastro zařízení, klimatizací, zemědělských strojů, tiskáren a obecně servisním a revizním technikům z oblasti elektro, voda a plyn. A co vidím jako velmi důležité, jde o produkt s předplatným v řádu stokorun na uživatele, na který snadno dosáhne malá firma i živnostníci.

NAŠE SERVISNÍ APLIKACE NEMÁ KONKUROVAT ROZSÁHLÝM ŘEŠENÍM TYPU SALESFORCE, ALE CHCEME JEJÍM PROSTŘEDNICTVÍM UKÁZAT, ŽE DIGITALIZOVAT OTRAVNÉ, ZDRŽUJÍCÍ A NA CHYBY NÁCHYLNÉ PROCESY MŮŽE OPRAVDU KAŽDÝ.

Po celou dobu jsme velmi intenzivně spolupracovali s prvním uživatelem aplikace, společností MARCCRAB GASTRO, které patří i naše poděkování za výbornou zpětnou vazbu.

TIP

DIGITALIZACE VYŽADUJE PŘEDEVŠÍM VŮLI A SNAHU NĚCO ZMĚNIT. KAŽDÁ APLIKACE ČI JINÝ NÁSTROJ JE PAK POUZE PROSTŘEDKEM, NIKOLI ŘEŠENÍM DIGITALIZACE.

4 Jak pomůže při poskytování servisních služeb umělá inteligence?

Ve Sprinxu technologii umělé inteligence zkoumáme opravdu intenzivně a servisní aplikace bude nejspíše prvním produktem, kde funkce podporované AI nasadíme. Plánujeme chatbota, který společně se zákazníkem zkusí odhalit nebo upřesnit příčinu problému. Pro servisní techniky připravíme funkci navrhující standardní postupy kontroly konkrétních zařízení a plánujeme i nasazení algoritmů na efektivnější plánování tras. První z těchto funkcí by se měly v servisní aplikaci objevit ještě do konce letošního roku.

5 Prozradíte nám ještě něco z dalších plánů?

Určitě se budeme soustředit na logistické funkce, konkrétně na optimalizaci času technika na cestě a na zakázce, abychom pomohli dispečerům efektivněji plánovat servisní zásahy. Chceme pracovat také s kvalifikací a schopnostmi techniků, aby dispečer vždy věděl, kdo se nachází blízko konkrétních zákazníků a s jakými zařízeními si poradí. ●

NÁSTROJ JAKO KAŽDÝ JINÝ

ŠTEFAN GOREJ

OBROVSKÝ ROZRUCH KOLEM KONVERZAČNÍ UMĚLÉ INTELIGENCE NÁS VE SPRINXU SAMOZŘEJMĚ NEMOHL NECHAT CHLADNÝMI. CHATGPT JSME DŮKLADNĚ OTESTOVALI A STÁLE PŘICHÁZÍME NEJEN NA NOVÉ MOŽNOSTI, KDE NÁM MŮŽE AI POMÁHAT, ALE TAKÉ NA ŘADU OMEZENÍ SOUČASNÝCH MODELŮ.

T Štefan Gorej, Radek Kubeš **F** Shutterstock, archiv

Vývoj kolem velkých jazykových modelů (Large Language Models – LLM), respektive konverzační umělé inteligence, nabral až neskutečnou rychlost. Takže je klidně možné, že ve chvíli, kdy čtete tento text, máte k dispozici ještě novější verzi služby ChatGPT s rozsáhlejší bází dat, ze které tato konverzační AI čerpá. Nebo třeba už pracujete s chatbotem Bard od Googlu, který si tentokrát nechal utéct cenné body za první místo v souboji s Microsoftem. Jedno je ale jisté, AI tu s námi je a bude a pronikne do stále více oblastí naší každodenní činnosti – bez ohledu na snahy o její regulaci.

AI PRO KAŽDÝ PŘÍPAD

Také ve Sprinxu samozřejmě konverzační AI intenzivně testujeme a přemýšlíme, jak tuto technologii využít při naší každodenní práci a ve prospěch našich klientů. Několik možností se vyloženě nabízí – kolega Honza Kotlín popisuje, jak s ChatGPT pracují v marketingu, dále můžeme AI využít při vývoji a testování softwaru a třeba také v HR – při výběru vhodných kandidátů nebo třeba individuálním vzdělávání. Naše dosavadní pokusy nás ale vedou k jasnému závěru – po fázi nadšení jsme došli k vystřízlivění. Současnou podobu konverzační umělé inteligence vidíme jako užitečný nástroj, který ale vyžaduje jasné vedení a také značnou zkušenost při jeho používání.

CHATGPT VÁS PŘEMÝŠLENÍ NEZBAVÍ

Když se poprvé bavíte s konverzačním botem poháněným umělou inteligencí, možná získáte dojem, že všechno ví, všechno zná a na všechno má odpověď. Ano, vypadá to tak. Ale když začnete pokládat hloubavější otázky a hlavně si výstupy ověřovat, asi budete zklamaní. Současná podoba AI má hned několik omezení – daných technologicky i uměle implementovaných tvůrci. Technologický limit spočívá v rychlosti, s jakou se jazykový model doplňuje o nové znalosti.

TIP

NEČEKEJTE NA PRVNÍ BEZPEČNOSTNÍ INCIDENT A CO NEJDŘÍVE STANOVTE, K JAKÝM ÚČELŮM A S JAKÝMI DATY MOHOU VAŠI LIDÉ JAZYKOVÉ MODELY TYPU CHATGPT PŘI SVÉ PRÁCI POUŽÍVAT.

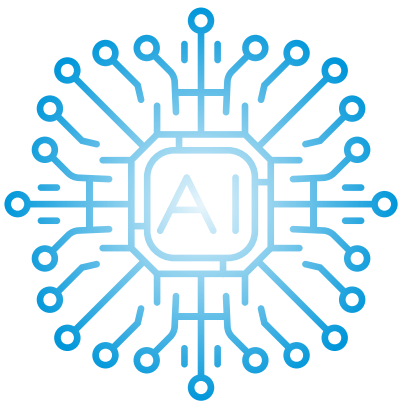
Umělá omezení pak představují určité etické hranice, které mají přinejmenším zkomplikovat možnost zneužití AI. Tyto limity je ale možné obejít.

Můžeme si uvést příklad. Pokud budete například začínající kyberzločinec a budete chtít po ChatGPT naprogramovat škodlivý kód, který po spuštění třeba zašifruje v počítači všechna data (tedy v podstatě ransomware), chatbot vám nevyhoví. Ale co když dáte AI roli softwarového vývojáře nebo kyberbezpečnostního experta a pak se velmi pečlivě formulovanými otázkami budete snažit odhalit slabiny v zabezpečení nějakého programu a zjistit, jakým způsobem je lze zneužít? To už vás AI neodmítne.

STEJNĚ JAKO DALŠÍ NÁSTROJE JE I UMĚLÁ INTELIGENCE DOBRÝM SLUHOU, ALE ŠPATNÝM PÁNEM. K AI JE VHODNÉ PŘISTUPOVAT S KRITICKÝM NADHLEDEM – NEJDE O VŠESPASITELNOU TECHNOLOGII, ALE O UŽITEČNÉHO POMOCNÍKA, KTERÉHO MUSÍME PŘI PRÁCI KONTROLOVAT.

NA CHYTROU OTÁZKU CHYTRÁ ODPOVĚĎ

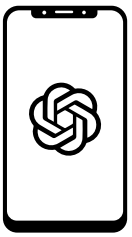
Výše uvedené směřuje k tomu, že při konverzaci s ChatGPT či jiným modelem AI je zcela klíčový způsob, jak otázky klademe – a také komu je klademe. ChatGPT může hrát různé role – třeba vám sepsat marketingový text ve stylu Aloise Jiráska, diskutovat s vámi jako jaderný fyzik nebo s vámi sehrát partii jako šachový velmistr.



To ovšem také znamená, že abychom byli pro umělou inteligenci rovnocenným partnerem, musíme o problematice, kterou chceme s pomocí ChatGPT či jiného modelu řešit, také něco vědět. I proto vnímám jazykové modely jako určité rozšíření našich biologických schopností. AI naše schopnosti podpoří, když nám poskytne rozsah znalostí v extrémně širokém kontextu, jaký dokáží (v daném čase) zpracovat pouze stroje. Proto je ChatGPT především doplněk, i když extrémně „chytrý" a užitečný, k našim vlastním myšlenkovým pochodům a intuici, který nám umožní překonat naše biologické limity. AI zkombinuje obrovské množství informací a nabídne závěry, které by nás možná nikdy nenapadly. Je ale na nás, abychom tyto výstupy dále použili s rozvahou a kritickým přístupem.

POZOR NA PUSU – AI NASLOUCHÁ

Stejně rychle, jako se lidé nadchli možnostmi modelu ChatGPT, vyvstaly i otázky bezpečnosti a regulace AI. Těžko říci, zdali a kdy se dočkáme nějaké regulace AI ze strany státu, respektive EU, nebo jak se budou vyvíjet a hlavně kontrolovat zmíněné „etické brzdy" implementované tvůrci modelů. Co ale vidím jako prakticky nezbytné, je nastavení pravidel využití konverzačních botů v rámci firem. Protože neznáme pozadí jednotlivých modelů, je nutné pečlivě zvážit, jaké informace budeme ChatGPT či jiné službě sdělovat a o jakých tématech se s AI budeme bavit. Ostatně podobným procesem jsme si již prošli při nástupu samotného internetu nebo později sociálních sítí – ty jsou také užitečným nástrojem, ale nesmíme se jimi nechat ovládnout. ●



NOVÝ KOLEGA V MARKETINGU

I když jsem se prozatím neodhodlal k pořízení placené verze služby ChatGPT, tu neplacenou už využívám velmi vydatně. V praxi se našemu marketingovému týmu osvědčilo využití AI například při komunikaci na sociálních sítích. Jazykový model zde může být velmi užitečný – například při boji s internetovým trollem, kdy dokáže přetvořit emotivní odpověď na korektní reakci. Stejně tak nám AI pomáhá navrhovat claimy pro kampaně na základě klíčových slov.

Můžeme si ušetřit i hodně manuální práce. Například jsme potřebovali vytvořit mutaci jednoho z našich webů do angličtiny. Měli jsme k dispozici soubor s desítkami řádků textu, který pro nás ChatGPT docela kvalitně přeložil. Stačily jen menší korekce a během chvíle jsme měli web přeložený. Takové využití bych určitě doporučil i našim zákazníkům, kteří obchodují ve více různých zemích.

Možnosti konverzační AI jsou opravdu zdánlivě nekonečné a záleží jen na nás, jak efektivně s nimi budeme schopni pracovat. Rozhodně ale platí pravidlo, že výstup bude jen tak dobrý, jak dobře je připravené zadání. Ostatně to samé platí i u lidí. Pak AI zvládne i velmi složité úkoly. Ale počítejte s tím, že pochopení principu a správné formulování zadání vám může zabrat i pár hodin. Kvalitním výstupem pak ale ušetříte ještě mnohem více času.

Jan Kotlín
Head Of Sales and Marketing

T Radek Kubeš **F** FraveBot

PO RAJČATECH A JAHODÁCH SE PUSTÍME DO OKUREK

VRATISLAV BENEŠ JE ZAKLADATELEM A ŘEDITELEM SPOLEČNOSTI OPTISOLUTIONS, KTERÁ SE ZABÝVÁ APLIKOVÁNÍM TECHNOLOGIE UMĚLÉ INTELIGENCE V PRŮMYSLU. SVOJE ZKUŠENOSTI S TECHNOLOGIÍ POČÍTAČOVÉHO VIDĚNÍ, SBĚREM A ANALÝZOU DAT, STROJOVÝM UČENÍM I AUTOMATIZACÍ VYUŽIL TÝM OPTISOLUTIONS K POSTAVENÍ REVOLUČNÍHO ŘEŠENÍ PRO PĚSTOVÁNÍ OVOCE A ZELENINY S PODPOROU INTELIGENTNÍCH, ROBOTICKÝCH TECHNOLOGIÍ.

Jak vznikla myšlenka na postavení pěstitelského robota?
Na začátku covidové pandemie jsme přišli o zákazníky z maloobchodu, a tak bylo více času věnovat se úvahám, jakým směrem se při vývoji našich produktů vydat. Shodou okolností začínalo léto, a jelikož doma pěstuji rajčata, nebylo už daleko k nápadu pomoci farmářům s pěstováním této oblíbené plodiny, která vyžaduje spoustu lidské péče. A tak vznikl náš projekt FraveBot – tedy FRuit And VEgetable roBOT – stejně jako samostatná firma FRAVEBOT.

Kam jste se s vývojem posunuli a co dnes FraveBot umí?
Pokud zůstaneme u rajčat, tak máme dnes v praktickém nasazení robota typu „scout", který projíždí mezi řádky rajčat ve skleníku a pomocí kamer se 4K rozlišením a analýzy obrazu kontroluje stav jednotlivých keříků. Díky znalostní bázi ve formě umělé inteligence dokáže náš FraveBot rozpoznat choroby rajčat a efektivně je ošetřit lokálním postřikem, zaštipovat boční výhonky a samozřejmě také kontrolovat velikost a zralost plodů. Tím se obrovsky šetří práce farmářům, kteří se mohou spolehnout na neúnavného pracanta. Ten nahradí několik lidí, kteří jinak musí každý den procházet skleníky a kontrolovat rostliny jednu po druhé. Pro srovnání – jeden člověk potřebuje na kontrolu hektarového skleníku asi 30 hodin času, zatímco FraveBot takovou plochu za stejnou dobu projede šestkrát. Typická velikost skleníku je u nás přitom 2 až 5 hektarů.

Jak je pro farmáře náročné takového robota nasadit a provozovat?
Jedním z našich hlavních cílů bylo, aby naši roboti nepotřebovali žádnou speciální infrastrukturu. Velkopěstitelské skleníky jsou dnes, podobně jako výrobní linky, vysoce standardizovaným prostředím s danými rozměry uliček, výškou záhonů nebo i rozměry kolejnic, na kterých se posouvají vozíky a po kterých může jezdit i náš robot. FraveBot je navíc plně autonomní, takže má baterii s výdrží na celou směnu, kterou lze snadno vyměnit za provozu, extrémně výkonný počítač na zpracování obrazových dat (kterých jsou tisíce gigabajtů denně) a také 5G modem, přes který se vytěžené znalosti odesílají do cloudu a jeho prostřednictvím do informačního systému pro farmáře. Naše roboty lze snadno servisovat a jejich programování probíhá kompletně na dálku.

Kde už FraveBot pracuje a jak je schopný spolupracovat s lidmi?
Naším pilotním projektem je podpora pěstování rajčat na rodinné farmě Ráječek. Její majitel Matěj Sklenář je pro nás obrovským zdrojem zkušeností s farmařením, bez kterého by ani vývoj našeho řešení nebyl možný. Za to jsme Matějovi a jeho farmě obrovsky vděční. A pokud jde o pohyb robota ve skleníku společně s lidmi, tak i zde jsme se rozhodli vydat úplně jinou cestou než současné farmářské stroje. FraveBot je vybavený lidarem, tedy radarem se schopností měření vzdálenosti. To znamená, že nemá klasické senzory nárazu a člověka či jakoukoli jinou překážku rozpozná už z velké vzdálenosti a včas se před ní zastaví. Takže na rozdíl od jiných autonomních strojů může FraveBot bezpečně pracovat společně s lidmi.

Soustředíte se jen na pěstování rajčat?
S rajčaty jsme začali, protože jde o mimořádně žádanou a z hlediska pěstování velmi lukrativní plodinu. A podobně jsou na tom i jahody. Takže jsme FraveBot, tentokrát už v plně digitálním modelu skleníku, naučili pečovat o keříky jahod a k tomu vyvinuli i dalšího robota, typu „harvestor", který umí jahody i sklízet. Pokud totiž jahody sbírají lidé a následně je třídí do krabiček, dochází k jejich zmáčknutí a plody se pak rychle kazí. To s naším robotem nehrozí, a navíc jsou jahody rovnou zváženy a ukládány do krabiček s odchylkou v řádu jednotek gramů hmotnosti.

> NASAZENÍ ROBOTA PRO FARMÁŘE NEZNAMENÁ, ŽE MUSÍ NAHRADIT JEDNOHO AGRONOMA TŘEMI PROGRAMÁTORY – FRAVEBOT SE PROGRAMUJE NA DÁLKU, PŘICHÁZÍ SE ZNALOSTNÍ BÁZÍ PRO KONKRÉTNÍ PLODINY A KAŽDÝM DNEM PRÁCE SE DÁLE ZDOKONALUJE.

TIP

S OHLEDEM NA KLIMATICKÉ ZMĚNY BUDE ZEMĚDĚLSTVÍ STÁLE NÁROČNĚJŠÍM OBOREM. DIGITALIZACE A AUTOMATIZACE POMŮŽE DO BUDOUCNA ZAJISTIT UDRŽITELNÉ PĚSTOVÁNÍ ZÁKLADNÍCH PLODIN.

Automatizace a AI už dorazily i do zemědělství.

Rajčata FraveBot nesklízí?
Nikoli, protože nejsou tak choulostivá jako jahody a lidé je (alespoň zatím) zvládnou sklidit mnohem rychleji než roboti. Zatím se tedy takové robotické řešení nevyplatí. U jahod ale umí FraveBot nejen informovat farmáře o aktuálním množství zralých plodů ke sklizni, ale třeba také přes noc posbírat přesně zadané množství jahod, které bude ráno připravené na rozvoz. Zatímco lidé zvládnou sklidit asi 20 kilo jahod za hodinu, FraveBot šetrně posbírá kolem 25 kilo – a samozřejmě dokáže pracovat celé hodiny bez přestávky.

Jaké jsou vaše další plány? Pustíte se do jiných plodin?
Jako první budeme nyní řešit logistiku – tedy odvážení sklizených plodů ze skleníku a také plně automatickou výměnu baterií v robotech. Z dalších plodin jsou ekonomicky zajímavé papriky a pak také okurky, které je nutné dodávat obchodníkům s velmi malou odchylkou velikosti a tvaru – a právě to by náš robot měl perfektně ohlídat. ●

Robotický zemědělec FRAVEBOT je robot, který usnadní agronomovi práci. Umí včas odhalit škůdce a choroby.

JAK CHRÁNIT DĚTI V KYBERPROSTORU?

T Jiří Jinger **F** archiv, Shutterstock

Do zabezpečení firemních dat a aplikací investujeme miliony, ale jak se staráme o to skutečně nejcennější – o bezpečnost našich dětí v online světě?

V kyberprostoru číhá na naše děti mnoho různých hrozeb, z nichž třeba nákupy her a bonusů z kreditky rodičů patří k těm nejméně nebezpečným. Určitě tak samo o sobě nestačí instalovat na počítače, mobily či tablety dětí antivirový software.

Co umí rodičovská kontrola?

Na každém zařízení, které děti používají, by měl být nasazen také nějaký typ rodičovské kontroly. Tím lze omezit jednak dobu používání zařízení a přístupu k internetu (na určitý čas nebo počet hodin denně), omezit instalaci a spouštění aplikací a her a samozřejmě také filtrovat internetové stránky. V případě mobilních zařízení umí rodičovská kontrola také zjistit aktuální polohu dítěte a zobrazit ji na mapě.

Základní funkce rodičovské kontroly (především ty spojené s internetem) jsou dnes součástí výbavy moderních Wi-Fi routerů, ale více funkcí a detailní přehled o aktivitách dětí nabídnou především pokročilá bezpečnostní řešení pro domácnosti nebo ještě lépe služby Google Family Link a Microsoft Family Safety, které jsou pro rodiče velmi snadno ovladatelné, a navíc jsou k dispozici zdarma.

Kyberšikana a další hrozby

K nejzávažnějším kybernetickým hrozbám, před kterými je potřeba děti chránit, patří kyberšikana, vydírání nebo sexuální predátoři. Děti si běžně zakládají účty na sociálních sítích a baví se s ostatními přes komunikátory nebo chat v různých hrách. Rodičovská kontrola ale dokáže tyto aktivity ohlídat pouze na úrovni zákazu konkrétních aplikací a webových stránek, nikoli podle obsahu.

Je třeba si uvědomit, že děti, jakkoli jsou v online aktivitách často daleko před svými rodiči, vnímají soukromí zcela jinak než dospělí a na sociálních sítích sdílí obsah, který by měl zůstat soukromý. Proto je především na rodičích, aby se zajímali o online aktivity dětí a bavili se s nimi o rizicích komunikace na internetu a důležitosti ochrany soukromí – to žádný software nenahradí. ●

TIP

ÚPLNÝM ZÁKLADEM BEZPEČNOSTI DĚTÍ NA INTERNETU JE UPŘÍMNÝ ZÁJEM RODIČŮ O JEJICH ONLINE AKTIVITY.