platform of invention

Informačné technológie pre podnikanie s nápadom

online | pdf | print

Užitočné v správnych hlavách

magazín pre CTO, CFO, CEO

číslo 6
ročník tretí | 2/2023

Kybernetická bezpečnosť

Pre fungovanie 24/7

Revolúcia v automatizácii firemných procesov

Rozumiete M365? Čo dokáže vzdelávanie vo vlastnej firme

Pomôže vám náš tím

Magazín o informačných technológiách

Tlačená aj elektronická verzia zadarmo.
Kliknite na tlačidlo a čítajte.

nové číslo

Čítajte 6. číslo
Venované téme kybernetickej odolnosti a IT vzdelávaniu zamestnancov.

PDF magazín | Online portál

Staršie čísla vo formáte PDF

#5

#4

#3

#2

#1

platform of invention
Informačné technológie pre podnikanie s nápadom

Magazín s ambíciou ukázať ako IT technológie ul'ahčujú firmám každodenný život, prinášať úspešné biznis riešenia, unikátne inovácie a trendy v IT, a pomáhať v uplatnení podnikatel'skej tvorivosti a invencie.

Výzva pre všetkých CEO, CTO a CFO

Ponúknite nám svoj príbeh využitia IT vo vašej firme a my vám bezplatne ponúkneme exkluzívnu možnosť prehovoriť do publika slovenský firiem.

Chcete zistiť viac a zapojiť sa?

Navštívte náš web, vyberte si vhodnú rubriku a odošlite formulár.

www.platformofinvention.sk/profil-magazinu/

klikni alebo oskenuj QR

Čítajte nás online!

Kompletný obsah platform of invention s rozšíreným obsahom a ďalšími článkami nájdete v elektronickej podobe magazínu.

www.platformofinvention.sk

klikni alebo oskenuj QR

EDITORIÁL

Úspech je výsledok tímového úsilia

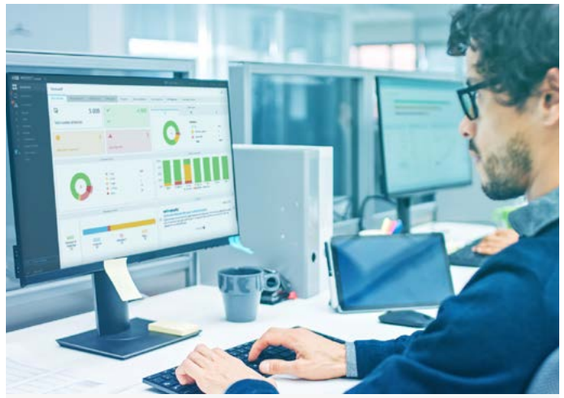
V neustále sa vyvíjajúcom prostredí kybernetickej bezpečnosti je najväčšou devízou spoločnosti jej špecializovaný tím odborníkov. V spoločnosti GAMO chápeme, že synergia medzi našimi zamestnancami je základom nášho úspechu, pretože sa snažíme neustále inovovať a riešiť naliehavé problémy. Vďaka viac ako 30 rokom spoľahlivých IT služieb pre verných aj nových zákazníkov je jasné, že naše úspechy sú skôr výsledkom tímového úsilia než práce jednotlivca.

Ponuka špičkových riešení a služieb si vyžaduje bezproblémovú spoluprácu rôznorodého tímu: špecialistov, analytikov, konzultantov, obchodníkov, projektových manažérov, operátorov helpdesku, ako aj neoceniteľnú podporu ekonomického a marketingového oddelenia. Každý člen tímu zohráva kľúčovú úlohu a naša spoločná sila spočíva v jednotnosti.

A naši obchodníci sú často prvými, ktorí reagujú na potreby zákazníkov. Rada by som vám preto predstavila časť obchodného tímu: Janu Kohárovú, Martinu Kormaník a Branislava Luptáka, ktorí hrdo reprezentujú značku GAMO v tomto vydaní Platform of Invention. Hoci sú neustále v pohybe, buď na cestách za klientmi, alebo s telefónom na uchu, uvedomujeme si, že v rýchlo sa meniacom kyber svete je najdôležitejšie zostať informovaní a vzdelaní. Vážime si chvíle, keď sa počas pracovného dňa máme možnosť stretnúť, či už je to neformálna káva v kuchynke, rýchly obed, alebo dokonca fotenie na titulku. Tieto interakcie sú príležitosťou na zdieľanie osobných aj profesionálnych skúseností, ktoré nás inšpirujú, povzbudzujú a poháňajú vpred.

V tomto podpornom prostredí pristupujeme aj k našim spoločným vzdelávacím aktivitám a školeniam. Uvedomujeme si, že oblasť kybernetickej bezpečnosti je poznačená rýchlym technologickým pokrokom, neustále sa vyvíjajúcimi trendmi, novými funkciami a potenciálnymi nástrahami. Preto je nevyhnutné, aby všetci členovia tímu GAMO zostali ostražití a dobre pripravení riešiť výzvy a príležitosti, ktoré sú pred nami.

Zuzana Omelková
Obchodná riaditeľka
zuzana.omelkova@gamo.sk



So zaplátaním zraniteľností si poradí ESET

Pre firmy je z hľadiska bezpečnosti kriticky dôležité ustrážiť, aby bol každý softvér aj operačný systém aktualizovaný na najnovšiu verziu. Mnohé aplikácie totiž obsahujú v určitom čase bezpečnostné chyby, takzvané zraniteľnosti, cez ktoré sa útočníci dokážu nabúrať do celej siete. Jediný spôsob ako zraniteľnosti opraviť je prostredníctvom aktualizácie. Preťažené IT tímy však často odsúvajú nasadzovanie záplat na druhú koľaj. Dobrou správou je, že firmy môžu túto časovo náročnú úlohu zveriť do rúk bezpečnostnému riešeniu. Nástroj **ESET Vulnerability & Patch Management** kontroluje tisícky populárnych aplikácií na prítomnosť viac ako 35-tisíc zraniteľností. Riziká je možné filtrovať a priorizovať podľa ich závažnosti. Firmy môžu uprednostniť opravu kritických chýb a zvyšné opravy naplánovať na čas mimo špičky, aby sa vyhli prerušeniam.

Článok pokračuje na platformofinvention.sk
klikni alebo oskenuj QR

Igor Kmiť
PR Specialist Slovakia
ESET, spol. s r.o.

Dôveryhodná cesta kybernetickej ochrany? To je Veeam. Aké má vylepšenia?

Zo štúdie Veeam 2023 Ransomware Trends Report vyplýva, že 93% útokov ransomvéru je zameraných na zálohy, pričom 75% týchto útokov je aspoň čiastočne úspešných. Ak sa hekerom podarí vymazať alebo zašifrovať záložné dáta, je pravdepodobnejšie, že organizácia zaplatí výkupné. Odborníci na IT a kybernetickú bezpečnosť vedia, že kritickou súčasťou stratégie kybernetickej odolnosti musí byť dôveryhodná, čistá záloha, ku ktorej má firma prístup kedykoľvek a odkiaľkoľvek.
Aktualizácia Veeam Data Platform 23H2 umožňuje radikálne zvýšiť odolnosť - nielen zotaviť sa po výpadku alebo strate údajov. Vďaka zabezpečeniu čo najkratšieho času medzi incidentom a obnovou môžu zákazníci udržať svoje podnikanie v chode a napredovať. Platforma obsahuje nové funkcie zabezpečenia a ochrany pred ransomvérom pre riešenia Veeam Backup & Replication™, Veeam ONE™ a Veeam Recovery Orchestrator, a je netrpezlivo očakávaná už aj na Slovensku. Aké vylepšenia prináša?

Článok pokračuje na platformofinvention.sk
klikni alebo oskenuj QR

Michal Štětina
Field Marketing Manager CEE
Veeam

Predčasný koniec Aktu o umelej inteligencii?

V júni 2023 sa viac ako 150 významných európskych spoločností, vrátane Renault, Heineken, Airbus či Siemens, podpísalo pod kritický otvorený list smerom k Európskej únii. Podľa nich návrh Aktu o umelej inteligencii v jeho aktuálnom znení môže eliminovať príležitosť, ktorú technológia AI poskytuje Európe, aby sa „opäť pripojila k technologickej špičke“. Signatári tvrdia, že regulatórne pravidlá sú príliš extrémne a hrozí, že namiesto toho, aby poskytli vhodné prostredie pre inovácie v oblasti AI, naopak, podkopú technologické ambície EÚ. Podľa návrhu Aktu o umelej inteligencii budú musieť poskytovatelia základných modelov umelej inteligencie – bez ohľadu na ich zamýšľané použitie – zaregistrovať svoj produkt v EÚ, podrobiť sa posúdeniu rizík, a splniť požiadavky na transparentnosť, napríklad zverejniť všetky údaje chránené autorskými právami, ktoré sa použili na trénovanie ich modelov. V otvorenom liste sa uvádza, že spoločnosti vyvíjajúce tieto základné systémy AI by boli vystavené neprimeraným nákladom na dodržiavanie predpisov a rizikám súvisiacim so zodpovednosťou, čo môže poskytovateľov AI podnietiť k úplnému stiahnutiu sa z európskeho trhu.

Táto kritika má zrejme – aspoň čiastočne – vecné opodstatnenie, čo potvrdzujú ostatné udalosti v legislatívnom procese.

Článok pokračuje na platformofinvention.sk
klikni alebo oskenuj QR

JUDr. Tomáš Klinka, JUDr. Štefan Pilár, JUDr. Peter Komínek
SIGNUM legal s. r. o.
advokátska kancelária

Digital Twin je ideálny partner pre kvalitný život

Digitálne dvojča predstavuje moderné IT riešenie umožňujúce efektívne riadiť procesy a prevádzku malých aj veľkých spoločností či monitorovať prostredie, v ktorom zamestnanci pracujú a trávia podstatnú časť ich životov. Ide o digitálnu kópiu akéhokoľvek objektu, nech už je ním čokoľvek – výrobná hala, parkovací dom, pohyb osôb alebo tovarov v logistike či strojov v priemysle.

GAMO a.s. nasadilo digitálne dvojča vo svojom sídle s cieľom vytvoriť ideálne pracovné prostredie pre svojich zamestnancov predpokladajúce komfortný pracovný výkon. Toto inovatívne riešenie vyžadovalo inštaláciu 15 senzorov na meranie CO2, vlhkosti a teploty, a dvoch senzorov na meranie elektrických veličín. Senzory sú prepojené s IoT zariadeniami a procesmi, ktoré zrkadlia fyzické priestory firmy digitálne v aplikácii Twinzo. Technológia tak umožňuje získavať relevantné informácie o pracovnom prostredí v reálnom čase a následne robiť pružné rozhodnutia na zabezpečenie ideálneho fungovania kancelárií a miestností na porady. Riešenia na mieru dokáže GAMO ako partner vývojovej spoločnosti Twinzo a dátovej spoločnosti T-Industry implementovať a koordinovať v akýchkoľvek priemyselných či kancelárskych priestoroch.

Článok pokračuje na platformofinvention.sk
klikni alebo oskenuj QR

Branislav Lupták
Obchodný manažér
GAMO a.s.

Je čas sa včas zorientovať pre firemnú analýzu rizík

Rok 2024 stavia zodpovedné firmy pred požiadavku preukázateľne prijať technické aj prevádzkové opatrenia v oblasti kybernetickej a informačnej bezpečnosti. Tie vyplývajú z legislatívy európskej smernice NIS 2. Budú možno platiť aj pre vašu firmu. Ide o požiadavky riadenia rizík, personálnej bezpečnosti a riadenia prístupov, bezpečnosti sietí a prevádzky informačných systémov, a v čase aj povinnosti absolvovať audit v oblasti kybernetickej bezpečnosti.

O čo presne ide?

Vyhláškou (362/2018), platnou od septembra 2023, je definovaný zoznam požadovaných bezpečnostných opatrení, ktoré budú pre firmy spadajúce pod smernicu NIS 2 povinné.
Aj napriek tomu, že doposiaľ nie sú presne vymenované sektory a veľkosť firmy s povinnosťou riadiť sa touto vyhláškou, je odporúčaním špecialistov na kyberbezpečnosť to, aby si subjekty vo vlastnom záujme a s predstihom zrealizovali aspoň analýzu rizík. Vykonajú tak dôležitú identifikáciu firemných

procesov a systémov, a zároveň získajú čas na odstránenie zraniteľností, ktoré by mohli mať dopad na fungovanie a chod firmy v dôsledku kybernetických incidentov.

Článok pokračuje na platformofinvention.sk
klikni alebo oskenuj QR

Martin Ondrušek
Manažér informačnej bezpečnosti
GAMO a.s.

Kybernetická bezpečnosť pre fungovanie 24/7

Kybernetická odolnosť, online ochrana spoločnosti a hospodárstva, sú jednou z priorít Európskej únie a každej zodpovednej krajiny. Pre zdravé fungovanie 24/7 je však nevyhnutné prijímať pravidlá správneho správania sa zdola. Od jednotlivých segmentov, firiem, ich vedúcich pracovníkov, po každého jedného zamestnanca.

O potenciálnych hrozbách a proaktívnych rozhodnutiach hovoríme so Zuzanou Omelkovou, obchodnou riaditeľkou a expertkou na kybernetickú bezpečnosť GAMO a.s.

Aké jednoduché je pre kybernetického zločinca hacknúť nezabezpečený subjekt?

Ako vojsť otvorenými dverami. V priemere 1 hodina a 42 minút stačia na to, aby sa útočník po hacknutí jedného zo zariadení spoločnosti dostal do zvyšku firemnej siete. Napadnutá firma pritom ani netuší, že má v systéme narušiteľa, ktorý sa môže v systéme tajne ‚prechádzať" a oficiálne nič nespraviť. Počas nasledujúcich týždňov či mesiacov si spoločnosť vôbec nemusí všimnúť, že je hacknutá.

Menia sa spôsoby útokov rokmi?

Áno, neustále sa prispôsobujú technologickému pokroku, zmenám v digitálnom prostredí a zlepšeniam v oblasti kybernetickej ochrany. Kyberzločinci sú motivovaní hľadať nové vektory a techniky útoku, aby obišli bezpečnostné opatrenia a dosiahli svoje kriminálne ciele. Ale máme aj výnimky, ktoré pretrvávajú desaťročia. Zmenila sa však taktika, rozsah a dopad na ich obeť. Táto dynamická povaha kybernetických útokov zdôrazňuje dôležitosť neustálej aktualizácie a zlepšovania opatrení kybernetickej bezpečnosti na ochranu pred vznikajúcimi hrozbami.

Aký vývoj kybernetických útokov možno v roku 2024 očakávať?

Predvídať konkrétne kybernetické útoky v budúcnosti je náročné práve pre rýchlo sa vyvíjajúcu povahu hrozieb kyberbezpečnosti. Niekoľko všeobecných trendov a typov kybernetických útokov, ktoré budú pravdepodobne pokračovať alebo sa objavia v nasledujúcich rokoch, však môžeme predvídať. Jednou z hlavných kybernetických hrozieb je stále ransomvér. Ďalej to môžu byť útoky zamerané na rastúci počet zariadení internetu vecí (IoT), kvantové počítačové hrozby, ktoré môžu mať potenciál prelomiť súčasné šifrovacie algoritmy. Využívaním umelej inteligencie a strojového učenia môžu byť deepfake útoky a spear-phishing oveľa presvedčivejšie.

Ako sa im vedia spoločnosti vyhnúť?

Keď subjekt čelí narušeniu nejde len o problém IT, ale o závažný celofiremný problém. Prvým krokom k úplnej ochrane firmy je skutočné pochopenie vplyvu narušenia alebo útoku na podnikanie, ako aj hodnoty proaktívnej iniciatívy v oblasti kyberbezpečnosti. S proaktívnym myslením môžete prijímať rozhodnutia potrebné na úplnú ochranu firmy.

Odporúčame každému držať krok s narastajúcimi nárokmi: či už legislatívy a štandardov kybernetickej bezpečnosti, s vývojom IT technológií, ale aj so samotnými hrozbami. Obchodný úspech každej zodpovednej spoločnosti dnes priamo závisí od úrovne zabezpečenia a pripravenosti na krízové situácie. Pohnúť sa z bodu nula a uvedomiť si vlastnú zraniteľnosť je často najťažšie. Ako prvé je dôležité poznať mieru ohrozenia aspoň v hrubých rysoch, to znamená vykonať prinajmenšom posúdenie stavu kybernetickej odolnosti a analýzu rizík.

Podľa štatistík je však 95% úspešných kybernetických útokov spôsobených zlyhaním ľudského faktora. Tu sú všetky zabezpečenia zbytočné?

Určite nie. Nasadenie bezpečnostného riešenia je účinné vtedy, ak je podporené v danej problematike uvedomelými zamestnancami so schopnosťou kriticky myslieť a dodržiavať zásady ochrany firemnej aj súkromnej identity a tímlídrami so schopnosťou vyhodnocovať riziká a na základe nich implementovať bezpečnostné opatrenia s cieľom udržania biznis kontinuity firmy. V oboch prípadoch treba byť obozretný, všímať si maličkostí, a neprehliadať detaily.
Zvyšovanie povedomia tímov v oblasti kybernetickej bezpečnosti školeniami je súčasťou zdravej firmy.

Čo možno rozumieť pod preventívnou ochranou v praxi?

Ide o prípravu na to, čo môže prísť. Venujeme sa prevencii a tréningu, aby sme sa vedeli chrániť pred rôznymi typmi útokov. Čím sme odolnejší voči týmto útokom, tým menej sú naše dáta a informácie vystavené nebezpečenstvu. V mnohých prípadoch z vykonaných analýz a testov vyplýva, že množstvo zistených nedostatkov a zraniteľností je možné odstrániť bez veľkých investícií, napríklad už len pravidelným aktualizovaním systémov. Jednoducho povedané: stačí mať úprimnú snahu a záujem riešiť kyberbezpečnosť bez toho, aby to niekto prikazoval. Dostať sa z reaktívneho prístupu na proaktívny.

Aké formy ochrany poskytuje GAMO klientom?

Poskytujeme komplexné služby, prostredie aj znalosti, k adekvátnemu zareagovaniu a odolávaniu potenciálnym kybernetickým útokom.

Dôležitou súčasťou našej stratégie je testovanie zraniteľností. Zjednodušene ide o skenovanie a systematickú identifikáciu slabých miest vo firemných systémoch, sieťach a aplikáciách, ktoré by mohli byť zneužité útočníkmi.

Následne vykonávame implementáciu bezpečnostných nástrojov, preberáme starostlivosť o bezpečnostný monitoring, detekciu a reakcie na incidenty v rámci poskytovanej SLA služby – všetko podľa potrieb zákazníka, s odbornými znalosťami a skúsenosťami.

Samozrejme, must have je prvotná analýza IT prostredia a už spomínané školenia radových zamestnancov, IT oddelení či tímlídrov.

Môže byť stav odolnej firmy v kybernetickom priestore trvalo udržateľný?

Áno, mohol by, pri dodržiavaní všetkých odporúčaných bezpečnostných opatrení plus sledovaní nových trendov. Špecialisti kybernetickej bezpečnosti nie sú zárukou toho, že vás útočníci nenapadnú, ale sú predovšetkým expertmi na riziká, ktoré prostredníctvom bezpečnostných opatrení eliminujú.

Odporúčame preto každému držať krok s narastajúcimi nárokmi: či už legislatívy a štandardov ohľadom kybernetickej bezpečnosti, alebo s vývojom IT technológií pre efektívnejšie výrobné procesy. Čas a pripravenosť, to sú dnes nielen v kyber priestore kľúčové heslá.

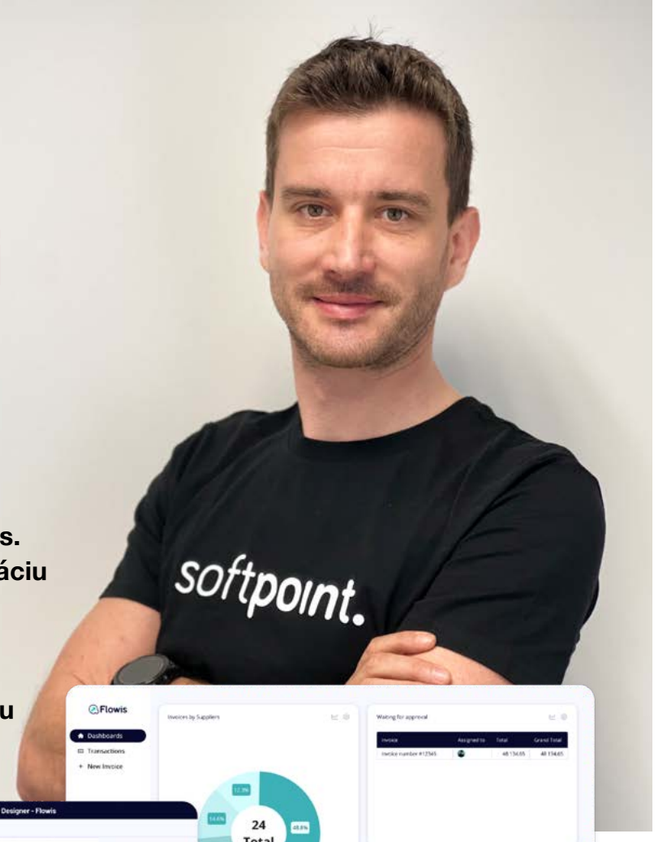
Článok čítajte na platformofinvention.sk

Klikni alebo oskenuj QR

Iveta Hlaváčová
iveta.hlavacova@gamo.sk

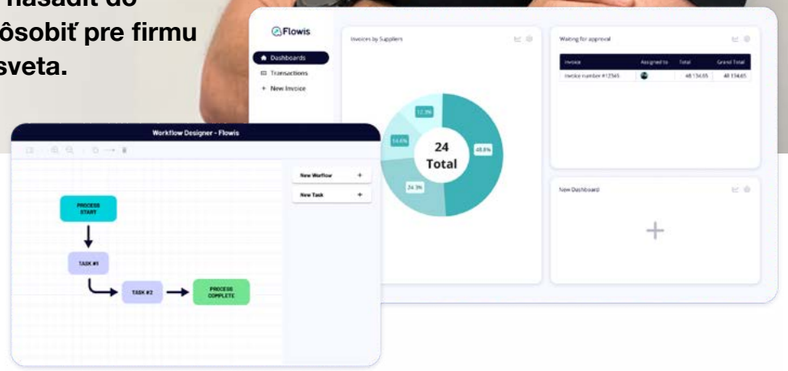
SUCCESS STORY

Revolúcia v automatizácii firemných procesov



SoftPoint s.r.o. v úzkej spolupráci s GAMO a.s. implementovali svoju aplikáciu na automatizáciu a riadenie fakturačných tokov Flowis v nadnárodnej korporácii Johnson Controls. Aplikáciu sa podarilo úspešne nasadiť do cloudového prostredia a prispôsobiť pre firmu pôsobiacu až v 160 krajinách sveta.

Peter Jakubík, konateľ SoftPoint s.r.o.



Multitenantná platforma priniesla doslova revolúciu v riadení finančných procesov nadnárodnej korporácie. Revolučná technológia tak úplne zmenila doteraz zaužívaný spôsob spracovania faktúr.

Inovatívne riešenie umožňuje veľkým korporáciám, ale aj menším a stredným firmám, automatizovať a štandardizovať svoje finančné procesy. Jedna verzia aplikácie umožňuje efektívne a bezpečné zdieľanie rovnakých zdrojov a slúži viacerým klientom súčasne. Každý klient má pritom prístup k vlastným konfiguráciám a údajom. Dnes automatizuje daná aplikácia spracovávanie viac ako 200-tisíc faktúr mesačne, pričom aktívne ju využíva cez 12 000 používateľov.

„Chceli sme naplniť očakávania klienta, preto sme hľadali partnera, ktorý by nám pomohol navrhnúť architektúru aplikácie a vytvoril pre ňu spoľahlivé, flexibilné a bezpečné prostredie v Microsoft Azure," hovorí **Ing. Peter Jakubík**, konateľ spoločnosti SoftPoint, s.r.o.

Predchádzajúce pozitívne skúsenosti s poskytovaním licencií Microsoftu preto priviedli SoftPoint k spolupráci so spoločnosťou GAMO. Napriek tomu, že takto rozsiahlu implementáciu predtým nikdy nerealizovali, nasadili GAMO inžinieri spolu s projektovým tímom SoftPoint aplikáciu do cloudového prostredia úspešne.

Ako prvé vytvorili dve samostatné inštalácie kubernetov v Azure cloude. Jedna mala testovať aplikáciu, ďalšia vytvorila produkčné prostredie, pričom obe zahŕňali konfiguráciu kubernetov, storage, vytvorenie a nastavenie databáz, SSL certifikátov, sietí, backupov, a nastavenie základného monitoringu prostredia.

Nato nasledovalo finálne doladenie a príprava na ostrú prevádzku pre koncového klienta.

„Nebolo to jednoduché, museli sme sa prispôsobiť požiadavkám klienta, možnostiam cloudového prostredia, aj našim schopnostiam. Nakoniec sme však vďaka úzkej spolupráci so špecialistami z GAMO odladili funkčnosť aplikácie na maximálnu možnú úroveň," objasňuje Peter Jakubík. „Naučili sme sa pritom používať cloudové prostredie do takej miery, že si ho dnes už vieme spravovať samostatne, vlastnými kapacitami."

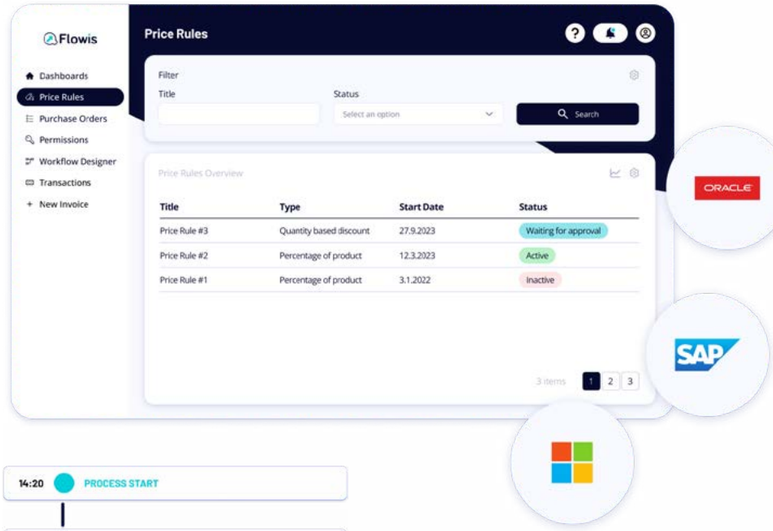
Po úspešnej implementácii u prvého veľkého klienta sa Flowis rozšíril aj do ďalších troch nadnárodných korporácií a desiatok menších a stredných firiem po celom svete. Vďaka výnimočnej konfigurovateľnosti si každá organizácia dokáže prispôsobiť platformu, a tým aj firemné procesy svojim vlastným potrebám.

A čo prináša Flowis v praxi?

Automatizácia v spracovaní faktúr

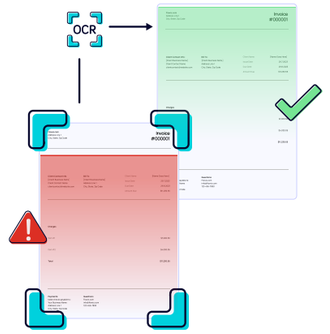
Nasadením do fakturačného systému Johnson Controls, kde sa mesačne spracúva približne 100 000 faktúr, umožnila integrovaná platforma plnú automatizáciu pracovných postupov, od prijímania a skenovania dokumentov, schvaľovania, účtovania, až po samotné platby. Zvýšila tak efektívnosť a jednotnosť celého procesu.

Aplikácia automatizuje proces čítania faktúr, ktoré prichádzajú do firmy v rôznych formách, využíva modely strojového učenia na extrakciu informácií, a prostredníctvom riadenia pracovných tokov zabezpečuje schvaľovacie postupy (automatické párovanie faktúr, objednávky a príjemky na sklade). Dôležitou súčasťou je aj automatizácia práce v rôznych účtovných systémoch a štandardizácia procesov. Tá zaručuje konzistentnosť schvaľovacieho procesu faktúr bez ohľadu na krajinu alebo účtovný systém.



Aktuálny celofiremný prehľad

Rýchlosť spracovania a validácie faktúr je kľúčovým prínosom. Faktúry, ktoré prechádzajú revolučným systémom, sú naskenované a zároveň zvalidované v priebehu jedného dňa. Validácia zahŕňa porovnávanie údajov na faktúrach s údajmi v účtovných systémoch, s cieľom identifikovať a vyčistiť duplicity či neúplné a chybné údaje alebo nesprávne ceny. Systém predstavuje podstatný nástroj



na sledovanie finančného vývoja firmy v období neustále sa meniacich cien materiálov a výrobkov. Umožňuje manažmentu pohotovo reagovať a aktívne riadiť ziskovosť. Funkcionalita aplikácie poskytuje okamžitý prehľad o stave faktúr, plánovanom cashflow, ako aj finančnej situácii celej organizácie.

Azure manažované služby sú kľúčové

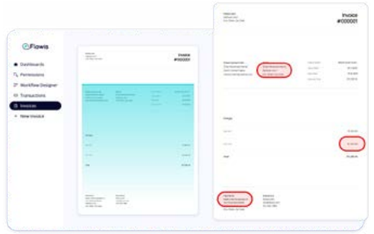
Flowis využíva Azure manažované služby ako rozhodujúcu súčasť svojej infraštruktúry. Zabezpečuje bezproblémový chod a správu systému. Azure Cloud so svojou flexibilitou a spoľahlivosťou poskytuje ideálny základ pre celosvetovú implementáciu. Kubernetes efektívne podporuje kontajnerizáciu a správu aplikácií, Postgres a Redis poskytujú spoľahlivé úložisko dát, zatiaľ čo Azure Storage umožňuje bezpečné ukladanie a zdieľanie informácií. Vďaka pokročilým technológiám je Flowis nielen vysoko výkonný, ale aj prispôsobivý meniacim sa potrebám firiem.

Viac než len faktúry

Aplikácia je významným pomocníkom firiem nielen v oblasti finančných procesov, ale aj v iných oblastiach podnikania, ako je napríklad riadenie ľudských zdrojov či riešenie reklamácií. Je schopná automatizovať rôznorodé firemné procesy. Flexibilita a výborná konfigurovateľnosť umožňuje firmám prispôsobiť si platformu vlastným potrebám a pristúpiť ku komplexnej automatizácii. Dynamické a inovatívne podniky tak môžu maximalizovať efektívnosť, znížiť náklady, a dosiahnuť konkurenčnú výhodu. Flowis sa tak stáva doslova strategickým partnerom.

Low-code aj no-code

Revolúciu v možnostiach konfigurácie a implementácie integrovanej platformy Flowis priniesli inovatívne riešenia low-code a no-code, ktoré umožňujú zákazníkom aplikovať vlastné nastavenia bez veľkých technických znalostí. Vytvoril sa tak priestor pre kreativitu a rýchlosť vo vývoji, pričom každý si môže aplikáciu modifikovať podľa svojich potrieb. Vzdelávacia platforma Flowis University ponúka užívateľom možnosť získať technické znalosti a objavovať praktické tipy a triky pre optimálnu konfiguráciu aplikácie. Môžu tak odhaľovať jej potenciál a stať sa architektmi vlastného finančného prostredia.



Budúcnosť s Flowis

Pokroková technológia, no aj revolučný nástroj, ktorý mení systém a akým svet pristupuje k spracovaniu faktúr, je prísľubom efektivity, štandardizácie, aj globálnej transparentnosti vo firemných procesoch. Ako inovatívne, multitenantné riešenie sa neustále prispôsobuje potrebám firiem v oblasti finančných procesov. Poskytuje nielen vysokú efektívnosť, ale aj maximálnu flexibilitu pre klientov z celého sveta, ktorí hľadajú moderné a inovatívne riešenia.

Článok čítajte na platformofinvention.sk

klikní alebo oskenuj QR

Jana Kohárová
jana.koharova@gamo.sk

Elektronické colné konanie

Ak dovážate tovar zo zahraničia, rozhodne musíte mať na zreteli všetky povinnosti, ktoré s vysporiadaním importovaného tovaru súvisia.

Vstupom do Európskej únie sme sa stali súčasťou spoločného trhu bez vnútorných a colných hraníc medzi členskými štátmi. V praxi to znamená, že ak chcete dovážať tovar na Slovensko z niektorej členskej krajiny, môžete tak urobiť bez toho, aby ste potrebovali povolenie či museli následne platiť clo. V prípade importu tovaru z tretích štátov, teda krajín, ktoré nepatria do colnej zóny Európskej únie, sa na tento tovar uplatňujú colné predpisy a daňové povinnosti. Celý proces colného prerokovania Finančnej správy takejto zásielky je komplikovaný a zoberie vám nejednu hodinu z vášho času. K tomu sa zíde automatizovaný systém, zabezpečujúci elektronickú komunikáciu s Finančnou správou SR na vysporiadanie celého procesu colno-deklaračného konania.

Uvítate službu, ktorej cieľom je spracovanie zásielok z krajín mimo EÚ od ich vstupu do krajiny automatizovaným spôsobom, cez vybavenie náležitostí v rámci colno-deklaračného skladu až po prepustenie zásielky do voľného obehu, ako aj odoslanie údajov do externého systému pre potreby jej doručenia adresátovi a výber vyrubeného colného dlhu. Komplexné riešenie s množstvom integrácií, ktoré podporujú hlavný cieľ – elektronické colné vysporiadanie zásielky.

O tom, ako komplexné riešenie postupne implementovala a využíva Slovenská pošta, a.s., priblížime v nasledujúcom článku.

Tvorba a implementácia systému do prostredia klienta

V rámci projektu eCIP bol vedeniu Slovenskej pošty, a.s., na prelome rokov 2018/2019 predložený koncept riešenia elektronickej colnej deklarácie na zásielky z krajín mimo EÚ. Uvedený koncept obsahoval návrh na úpravu statusu Slovenskej pošty, a.s., ako colného deklaranta. Vedenie spoločnosti rozhodlo o nevyhnutnosti vytvoriť SW riešenie pre zabezpečenie zberu a konsolidácie dát o daných zásielkach, ako aj zabezpečenie zaručenej elektronickej komunikácie s IS FS SR (IS CEP). Na základe vykonaných analýz rôznych možností riešenia došlo k rozhodnutiu vedenia Slovenskej pošty, a.s., o vytvorení a implementácii samostatného modulu ECK (elektronické colné konanie) v rámci IS JSSA, ktorý už Slovenská pošta, a.s. používala na rôzne agendové spracovania v rámci spoločnosti. Na implementácii a konfigurácii JSSA-ECK začal dodávateľ, spoločnosť GAMO a.s., pracovať v roku 2019. Slovenská pošta, a.s., začala používať systém v rutinnej prevádzke od 1. 1. 2020 na elektronickú colnú deklaráciu zásielok v poštovom styku s obsahom obchodného tovaru s hodnotou vyššou od 22 EUR do 1 000 EUR. Systém ECK bol následne rozšírený aj o možnosť elektronickej komunikácie zákazníkov s colným deklarantom cez portál Slovenskej pošty.

Od 1. 7. 2021 došlo rozhodnutím Európskej komisie k zrušeniu bezcolného limitu 22 EUR a zároveň k zjednodušeniu procesu colnej deklarácie pri eCommerce zásielkach do hodnoty 150 EUR. Uvedená zmena viedla k niekoľkonásobnému navýšeniu počtu colne deklarovaných zásielok. Novej situácii sa muselo prispôsobiť aj ECK - nasadením funkcionality umožňujúcej automatizovanú colnú deklaráciu bez priameho zásahu colného deklaranta. Automatizácia procesu bola dosiahnutá čerpaním informácii k colnej deklarácii z dostupných colných dátových zdrojov a implementáciou strojového učenia pri jednoznačnej identifikácii tovarových položiek podľa colného sadzobníka. Vďaka tejto implementácii dokáže Slovenská pošta, a.s., deklarovať vysoké počty zásielok mesačne.

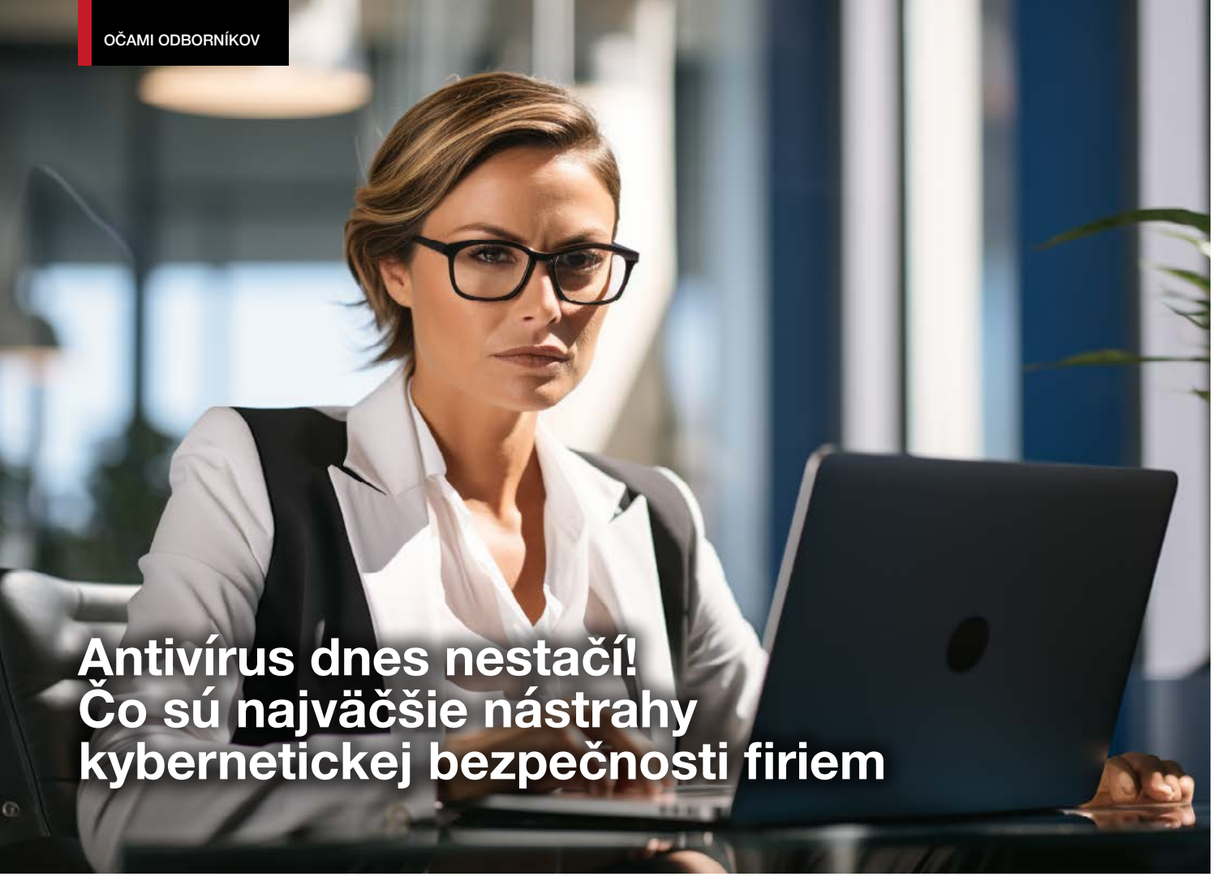
Ďalšie rozšírenie systému ECK bolo realizované na základe nových legislatívnych požiadaviek na colné konanie. Postupne bola implementovaná funkcionalita bezpečnostnej kontroly „Import Control System“ (ICS2). Zároveň sa systém ECK rozširuje aj o funkcionality, cielené na zvýšenie komfortu zákazníkom pri doručení zásielok z tretích krajín. Jednou z takých úprav je možnosť uhradiť všetky poplatky a DPH už pri nákupe tovaru v e-shope, vďaka čomu sa zjednoduší proces doručenia zásielky. S cieľom poskytnúť manažérom prehľadné informácie o colno-deklaračnom procese bude ECK rozšírené o Business Intelligence nástroj prehľadne zobrazujúci stav spracovania zásielok, ktorý rozšíri už implementovaný prevádzkový reporting.

Rozvoj systému a vízia komerčného uplatnenia

Nazbierané skúsenosti z doterajšej implementácie systému ECK plánujeme v GAMO do budúcnosti zužitkovať pri kompletizácii riešenia pre colné konanie s cieľom obsiahnuť všetky colno-deklaračné procesy pri dovoze, vývoze a tranzite, a to bez ohľadu na hodnotu a obsah zásielok. Zámerom je vytvoriť používateľsky prívetivé webové prostredie s maximálnym stupňom automatizácie procesov - vďaka implementácii strojového učenia, integrácii na medzinárodné siete a implementácii legislatívnych zmien - v dostatočnom predstihu. Systém bude umožňovať individuálnu, ale aj hromadnú deklaráciu tovarov a zásielok. Poskytovať bude preddefinované scenáre umožňujúce efektívnu deklaráciu vybraného tovaru, vďaka zobrazeniu len relevantných informácii pre daný typ. Súčasťou riešenia bude aj sprievodca procesom, ktorý uľahčí deklaráciu začínajúcim používateľom a pomocník obsahujúci všetky relevantné legislatívne informácie. V systéme bude možné definovať si vlastný workflow pre často opakujúce sa procesy, čím sa ešte viac zefektívni práca.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR

Martina Kormaník
martina.kormanik@gamo.sk



Antivírus dnes nestačí! Čo sú najväčšie nástrahy kybernetickej bezpečnosti firiem

Vedeli ste, že drvivá väčšina kybernetických útokov je zapríčinená práve ľudskou chybou a nedostatočnými vedomosťami zamestnancov? A incidentov neustále pribúda. Iba za prvý polrok 2023 vzrástol počet podvodných phishingových e-mailov na Slovensku trojnásobne.

Kým donedávna sa dali hrozby pomerne jednoducho odhaliť, a to aj vďaka zlej gramatike či nezrozumiteľnému kontextu, nástup umelej inteligencie spôsobil nárast kvalitnejších podvodných správ, s ktorými má čoraz väčšie problémy aj skúsený IT profesionál.
Produkty spoločnosti ESET len za šesť mesiacov odhalili a zablokovali tri často sa vyskytujúce hrozby:

- Falošné prihlasovacie okno HTML/Phishing.Agent, ktoré sa e-mailom distribuovalo ako HTML príloha a po otvorení v prehliadači imitovalo služby Microsoft Office ako je Outlook či SharePoint.
- E-mail DOC/Fraud sextortion, v ktorom útočník predstieral vlastníctvo chúlostivej sexuálnej nahrávky obete a žiadal sumu 1 500 EUR v bitcoinoch, aby video nezverejnil, pričom podľa ESET zaznamenal tento útok až 277 % nárast.
- A phishing, zneužívajúci značku Slovenská pošta, kde e-mailová správa informovala o vymyslenom doručení balíka po vyplatení fiktívneho colného poplatku. Podvod sa objavoval tento rok až o 275 % častejšie a postúpil tak v rebríčku phishingových hrozieb o sedem priečok vyššie.

O kybernetických nástrahách a z toho vyplývajúcej dôležitosti vzdelávania a osvety v oblasti kyberbezpečnosti firiem sme hovorili so špecialistom spoločnosti ESET **Júliusom Seleckým**, ESET Senior Technical Pre-Sales Representative.

Kybernetická bezpečnosť firiem je dnes v rukách nielen IT administrátorov, ale aj zamestnancov a vedenia firmy. Prečo sú osveta a vzdelávanie v tejto oblasti tak dôležité?

Bezpečnosť firmy stojí na troch hlavných pilieroch: ľuďoch, technológiách a procesoch. O dôležitých bezpečnostných otázkach vo firme by mali byť informovaní všetci - od pomocného personálu až po vrcholový manažment a odolnosť celej firmy sa tým značne zvýši. Ľuďom vo firme treba venovať rovnakú pozornosť ako bezpečnostnému softvéru či hardvéru a politikám. Ich vzdelávanie sa neraz zanedbáva, pritom práve ľudia sú najčastejším vektorom útokov. ESET svojich zamestnancov pravidelne interne školí napríklad aj v odhaľovaní podvodných phishingových e-mailov. Ak si pozrieme štatistiky, tak phishing, e-mail, ktorý sa snaží vylákať prístupové údaje alebo bankové údaje, je na popredných priečkach kybernetických hrozieb. Zamestnancov preto pravidelne testujeme odosielaním správ, ktoré sa tvária ako legitímne, avšak nie sú, a úlohou zamestnanca je podobnú falošnú správu odhaliť. Klientom zase ponúkame ESET tréning kybernetickej bezpečnosti, e-learningové kurzy, ktoré slúžia na všeobecné zvýšenie povedomia.

Kladú slovenské firmy dostatočný dôraz na kybernetickú bezpečnosť? Ako často je potrebné sa preškoľovať?

Život okolo nás je úzko naviazaný na informačné a komunikačné technológie a kybernetické incidenty oslabujú firmy, štát, respektíve celú ekonomiku a aj dôveru ľudí v tieto inštitúty. Bez posilnenia kyberbezpečnosti nie je možné napredovať, preto sa na ňu kladie stále väčší dôraz. Jednorazové školenie však veľký význam nemá, vzdelávať treba pravidelne, pretože ľudia potrebujú mať bezpečnosť stále na očiach, aby si ju zautomatizovali.

Vhodným formátom školenia je raz ročne základné, všeobecné školenie pre každého, kto vo firme používa PC. Plus počas roka potom ďalšie doplnkové školenia, napr. na jednotlivé témy IT bezpečnosti alebo zamerané na zamestnanecké role (IT administrátori, developeri, účtovné oddelenia, manažment atď.).

A najmä na čo by sa mali firmy v rámci vzdelávania zamestnancov v oblasti IT bezpečnosti zamerať?

Spoločnosť vyvíjajúca softvér sa bude sústreďovať na bezpečný vývoj, sieť hotelov zase na prevenciu fakturačných podvodov, priemyselné zariadenie na bezpečnú obsluhu OT atď. Riadenie ľudských rizík firmy by malo pozostávať zo súhrnu aktivít založených na dátach individuálnej organizácie a na odbornej analýze rizík, nie z kontextu vytrhnutých a chaotických reakcií na aktuálne buzzwordy.

Školenie je však iba jedna časť vzdelávania! Druhá, ešte dôležitejšia, je praktická skúsenosť. Je dokázané, že teória bez praxe je nanič. Napríklad aj zamestnanci, čo počuli o podvodných e-mailoch a vedia, že obsahujú podozrivý odkaz, doň pri prvom teste napíšu svoje údaje. Alebo pracovníci, ktorí počuli o manažérovi hesiel a vedia, že je vhodné ho využívať, ale iba tretina z nich to reálne robí.

Ako teda vysvetliť vedeniu spoločností nevyhnutnosť IT bezpečnosti podniku?

Rovnako ako sa používa uzamykanie dverí, nastavenie alarmu a kamery na ochranu fyzického priestoru, je kybernetická bezpečnosť to isté, len v digitálnom svete. Ak som ešte neinvestoval do týchto virtuálnych zámkov, budem vyzerať akoby som uviazol niekde v minulom storočí. V mnohých prípadoch ale zaberie až nepríjemná osobná skúsenosť, pričom obeťami útokov sa stávajú nielen bežní zamestnanci, ale aj vrcholový manažment.

Nedávno si útočníci cez platformu LinkedIn vytipovali konkrétnu spoločnosť a zamestnancovi ponúkli atraktívnu pracovnú pozíciu, pričom ak sa o ňu chcel uchádzať, musel vyplniť test, ktorý mu

Július Selecký, Senior Technical Pre-Sales Representative, ESET

poslali v určitom súbore. Keď ale súbor v práci otvoril, obsahoval nebezpečný škodlivý malvér a ten sa hneď po spustení dostal do firemnej siete, oskenoval ju, zistil koľko je zraniteľných počítačov a rozšíril sa ďalej. Týmto spôsobom sa útočníci dostali k firemným údajom. Keby bol dotyčný zamestnanec vyškolený, vedel by, že tento typ súboru nemá spúšťať na pracovnom počítači, ale v izolovanom priestore, a k podobnému incidentu by nedošlo.

Vieme teda pomenovať najväčšie súčasné kybernetické hrozby, na ktoré by si firmy mali rozhodne dávať pozor?

Prax ukazuje, že najčastejšie riziká, čo by malo zohľadniť aj vzdelávanie, sú sociálne inžinierstvo a phishing, neúmyselné úniky dát či slabé autentifikačné mechanizmy. Každý typ organizácie má iné riziká vyplývajúce z ľudského správania sa.

ESET na svojom informačno-vzdelávacom portáli Bezpecnevofirme.eset.com publikoval 10 najväčších kybernetických hrozieb, pričom na prvých priečkach sa umiestnili nástrahy ako nedôsledná správa firemných systémov, phishingové a iné podvodné správy, ransomvérové útoky a riziká spôsobené nárastom hybridnej práce. Pre bežných ľudí a domácnosti zriadil ESET portál Bezpecnenanete.eset.com.

Firmy často využívajú viacero rôznych serverov, ako napríklad poštový server, webový server, DNS, VPN ap. Ako ochrániť takéto zariadenia, resp. včas odhaliť ich slabiny?

Tu je dôležité implementovať systém na automatizované skenovanie zraniteľností, tzv. Vulnerability Assessment, ktorý aj ESET ponúka ako službu na ich vyhľadávanie a správu. Možno tak včas odhaliť slabiny v systémoch (serveroch), ktoré útočníci zneužívajú a snažia sa tak poškodiť firmu. Zákazník dostane správu s popisom zistených nedostatkov s ohodnotením ich závažnosti. Následne, po konzultácií s odborníkmi z ESET, odporučíme kroky na odstránenie zistených slabých miest. V tomto sa firmy môžu obrátiť aj na dedikovaného partnera ESET, akým je GAMO.

Tak, aby sa táto dodatočná vrstva ochrany dostala čo k najširšiemu počtu zákazníkov, rozhodli sme sa v ESET implementovať riešenie Vulnerability a Patch management aj do našich riešení na ochranu. Dokáže aktívne sledovať zraniteľnosti v operačných systémoch a bežných aplikáciách a umožňuje aj automatizované nasadenie záplat na koncových zariadeniach, ktoré sú spravované cez našu jednotnú platformu PROTECT.

Hybridná práca predstavuje po pandémii nový fenomén. Povedzme si ešte na záver niečo viac o hlavných rizikách, ktoré prináša.

Pre špecialistov na IT bezpečnosť ide o skutočnú výzvu. Hybridná práca, teda jeden deň práca v kancelárii, ďalší zas doma, so sebou prináša viaceré riziká ako sú problematická ochrana firemnej siete, zle zabezpečená sieť v domácnosti, či zlé zabezpečenie prístupov do firemných systémov z home-office. Vzniká tu aj vyššie riziko straty alebo krádeže zariadení, používanie súkromných zariadení na prácu, alebo vyššia pravdepodobnosť, že zamestnanec naletí phishingu. Pomôcť by mohlo napríklad šifrovanie celého disku na firemných zariadeniach, spoľahlivý bezpečnostný softvér na koncových zariadeniach s funkciou Anti-Theft, a opäť aj vzdelávanie zamestnancov.

Samozrejme, neexistuje nejaké 100 % riešenie, ktoré keď sa implementuje, tak môžete prehlásiť, že ste chránení. Väčšinou ide vždy o súbor komplexných opatrení, ktoré dokážu významnou mierou znížiť kybernetické riziká.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR

Gabriela Repatá
gabriela.repata@gamo.sk

Rozumiete M365? Čo dokáže vzdelávanie vo vlastnej firme

Zopnite si ruky tak, že prekrížite prsty oboch rúk. Všimnite si, ktorý palec máte navrchu. Následne urobte to isté, len s tým rozdielom, že navrchu budete mať palec opačnej ruky ako pri prvom pokuse.

Určite ste toto jednoduché cvičenie všetci zvládli. Zaregistrovali ste zmenu? Cieľom tejto úlohy je poukázať na rozdiel vo vynaloženom úsilí a koncentrácii. Ak musíme vykonať činnosť, ktorá je nová, nerobíme ju automaticky, nie je rutinnou. Určité činnosti vykonávame zvykovo, nepotrebujeme sa nad nimi veľmi zamýšľať. Keď ich máme však zmeniť, vyžadujú si naše plné sústredenie.

Nové postupy si musíme osvojiť, kým sa stanú rutinou. Musíme si ich jednoducho natrénovať. Mnohonásobne to platí pri práci s technológiami. Veľmi rýchlo sa vyvíjajú, pribúdajú tu nové funkcie, s ktorými sa musíme skôr či neskôr zžiť. V tomto článku sa podelíme o skúsenosti a zistenia, ktoré vzišli z interných školení zameraných na používanie aplikácií Microsoft 365, používané našou spoločnosťou viac než sedem rokov, a doplnené aj o poznatky získané u zákazníkov.

Počiatočný „guláš“ z množstva aplikácií, ktoré Microsoft 365 obsahuje, vyvoláva skôr chaos a nedôveru, možno aj preto sú používateľmi doslova ignorované. Výnimku tvoria asi len Office aplikácie, Outlook a Teams.

Na MS aplikácie sa môžeme pozrieť na základe ich charakteristík a zoskupiť ich do jednotlivých kategórii podľa účelu:

- Služby na vytváranie obsahu (Word, Excel, PowerPoint a iné);
- Služby na uchovávania resp. ukladanie obsahu (OneDrive, Teams, SharePoint);
- Služby na internú aj externú komunikáciu (Outlook, Teams a iné);
- Nástroje na riadenie, zadávanie a kontrolu úloh (Planner, To-Do, Project a iné);
- Nástroje na automatizáciu procesov a pravidelne sa opakujúcich činností (Power Automate a iné);
- Manažérske nástroje a prehľady na zisťovanie aktuálneho stavu alebo sledovanie prognóz či vyťaženosti ľudských zdrojov (Power BI, Fabric, Viva a iné);
- Bezpečnostné nástroje ochrany identít, zariadení, aplikácií, firemného know-how (Defender, Entra, Intune, MFA a iné);
- Aplikácie, ktoré priebežne pribúdajú spolu s rýchlo sa meniacimi trendami.

Je ich veľa, sú vzájomne prepojené, dajú sa používať kombinovane. Každou novou vlastnosťou, ktorú objavíme, si prácu uľahčíme. Typický je príklad obyčajného ukladania súborov. Štandardná situácia, kedy riešime dilemu: Kam vlastne dokument uložiť a prečo?

Predstavme si tri úložiská ekosystému Microsoft 365. Viete v čom sa líšia a kedy ktoré použiť? Spoznať ich vlastnosti, osvojiť si postupy ich správneho používania, vám uľahčí rozhodovanie a ušetrí čas.

- **OneDrive:** osobné úložisko používateľa. Používateľ prideľuje a spravuje prístup k vlastným dokumentom.
- **Teams:** každý člen skupiny v kanáli má k dokumentom prístup a úplne rovnaké práva.
- **SharePoint:** knižnica dokumentov. Prístup k dokumentom je riadený vopred definovanými pravidlami – politikami.

Vysvetlime si to na príklade skúsenosti zákazníka počas školenia: *„Keď pripravujem smernicu, jej draft si uložím u seba na OneDrive. Pripomienkovať a konzultovať s kolegami ju budem cez Teams a finálnu verziu uverejním na SharePoint do používania pre celú firmu.“*

Zjednodušene povedané: zásadný rozdiel medzi úložiskami ekosystému Microsoft 365 je v prístupoch a právach k dokumentom.

Viete že:
Každá zmena je zaznamenávaná v histórii dokumentu. História dokumentu je silný nástoj. Okrem zaznamenávania každej úpravy dokumentu tiež umožňuje ľubovoľnú verziu obnoviť, a tým sa vrátiť k niektorej predchádzajúcej verzii.

Ako sa trénuje IT firma v IT zručnostiach?

Ako všade, aj u nás je to s úrovňou znalostí aj s požiadavkami na školenia rôzne. Čo oddelenie, to iné postupy práce. Agenda každého kolegu má ťažisko v inej činnosti, preferuje a používa iné systémy či nástroje.

Zistili sme, že želanú efektivitu práce dosiahneme len vtedy, ak používatelia budú vedieť, čo všetko im nástroje M365 umožňujú a ako jednotlivé aplikácie používať v kontexte svojej práce.

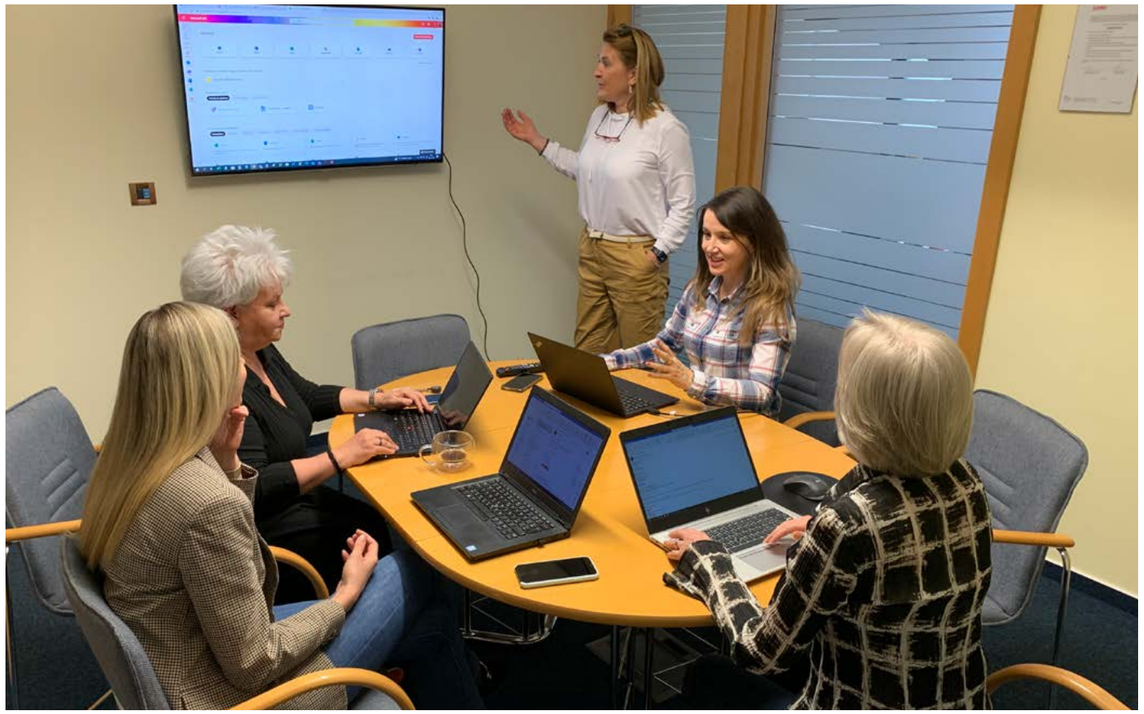
Ak chceme od kolegov, aby ich používali jednoducho a bezpečne, vysvetľujeme im „Prečo?“ by ich mali používať navrhovaným spôsobom a učíme ich „Ako?“ efektívne s nimi pracovať. Želaný stav dosiahneme, keď sami zistia, že prezentovaná výhoda, nová funkcia, zaujímavá „fičurka“, dáva zmysel a dokážu si ju rýchlo osvojiť a jednoducho používať.

Ako príklad uvedieme ukladanie cenových ponúk (ale aj iné typy súborov) do príslušnej skupiny v Teams. Prečo ukladať cenové ponuky do Teams? Lebo ak nie ste v práci, kolega (člen skupiny v kanáli), vás môže zastúpiť a cenovú ponuku dokončiť, zaktualizovať, upraviť. Ako? Možností je vždy niekoľko. Optimálne je používať tú, ktorá vyžaduje najmenej klikov, t.j. šetrí váš čas.

Osvedčená metóda vo vzdelávaní a tréningu používateľov M365 je venovať sa menším skupinkám, ktorých spája rovnaký alebo veľmi podobný charakter práce a spoločne s nimi nachádzať najvhodnejší postup na ich očakávania a požiadavky, súvisiace s využívaním aplikácií M365.

Často dopytovanou témou z realizovaných školení a tréningov, o ktorú sa používatelia zaujímajú, je prístup k uloženým dokumentom. Bez ohľadu na to, kde sa dokumenty nachádzajú (lokality Teams alebo SharePoint) pomocou synchronizačného klienta OneDrive, si ich dokážeme sprístupniť v Prieskumníku, automaticky aj v Total Commander.

Synchronizáciu dokumentov možno chápať ako „užívateľsky jednoduchší“ prístup k dokumentom, uloženým v cloud prostredí M365 (OneDrive, Teams, SharePoint), s možnosťou správy a riadenia priečinkov, lokalít a dokumentov.



Tipy k práci v OneDrive

Počas štyroch mesiacov v dvojtýždňových intervaloch väčšina našich zamestnancov absolvovala praktické cvičenia súvisiace s využívaním vybraných služieb Microsoft 365. „Ostrieľaní“ používatelia motivovali ďalších kolegov. Najsilnejšie rezonovala téma OneDrive a synchronizácie. Potvrdili nám to výsledky spätnej väzby - inšpirovať sa môžeme tým, čo ocenili naši kolegovia:

Zaujalo ma prepojenie Pozvánky na stretnutie - Nová schôdza so zošitom OneNote. Takto mám odkaz na zápis už priamo v pozvánke aj s prezenčkou. Počas stretnutia si viem písať poznámky a tiež odkliknúť, kto z pozvaných sa zúčastnil a kto nie.

Zmena v ukladaní všetkých dokumentov z pracovnej plochy na OneDrive, kde je k nim stály prístup a sú zálohované.

Praktickou funkciou je možnosť nastaviť si zálohovanie vybraných adresárov z lokálneho PC (napríklad Pracovná plocha) do OneDrive.

V rámci OneDrive mám veľa súborov a adresárov, ktoré zdieľam kolegom na zrevidovania alebo doplnenie informácií. A preto bola pre mňa zaujímavá informácia urobiť si raz za čas INVENTÚRU na OneDrive. Cez “Spravovať prístup - Manage Access” prehodnotiť aktuálnosť - odobrať prístup a zastaviť zdieľanie na dokumentoch, ktoré časom stratili význam pre zdieľanie.

Praktickou funkciou je uloženie dôležitej správy - konverzácie v MS Teams (doteraz som to nepoužívala, bola to pre mňa novinka, ale veľmi užitočná). Uložené komunikácie z rôznych kanálov, ktoré som si označila, nájdem týmto na jednom mieste.

Naučila som sa ako si dokážem rýchlo obnoviť omylom vymazaný dokument v Teams - zíde sa.

Čo vyjadruje Status pri synchronizácii?

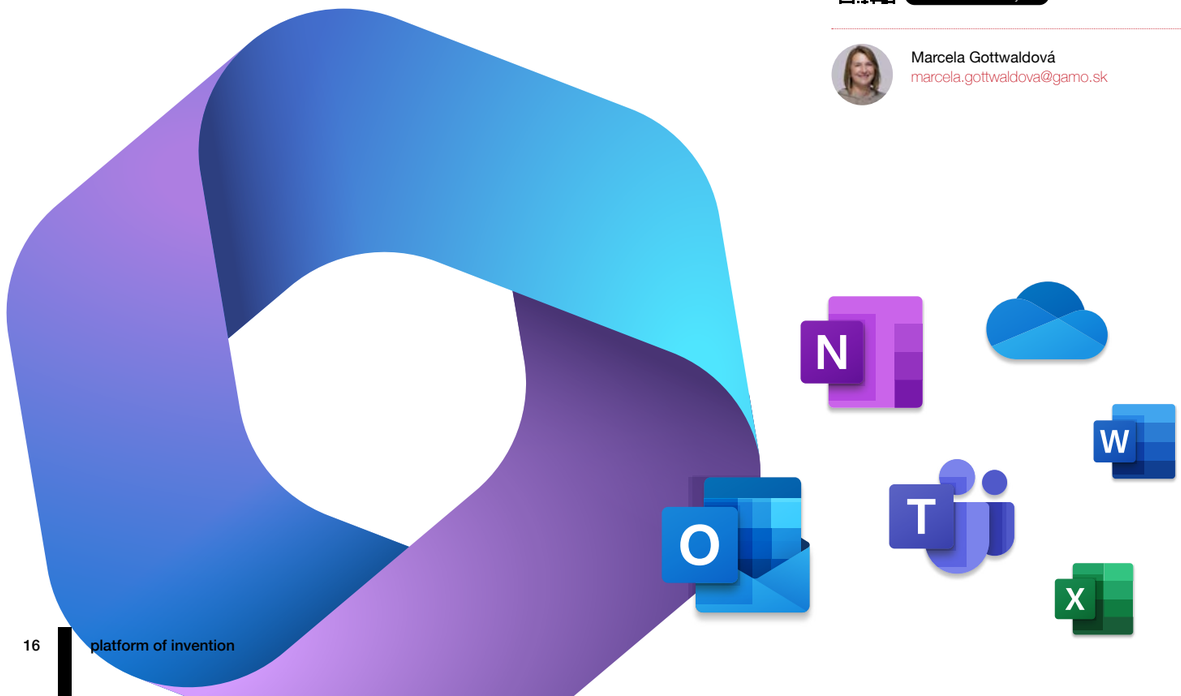
Modrý obláčik, zelená ikonka s plnou farbou, alebo ikona len s obrysom, označujú dostupnosť synchronizovaných dát. Priečinky a súbory môžu byť k dispozícii len v režime online alebo sú uložené lokálne v našom zariadení, vtedy k nim máme prístup aj v režime offline. Synchronizovaný obsah si dokážeme jednoducho spravovať a šetriť tak miesto na disku vo svojom zariadení ponechaním dokumentov v režime online. Vyskytujú sa však aj situácie, kedy je online režim nevyhovujúci. Potom máme možnosť dokumenty ponechať vo svojich zariadeniach a pracovať s nimi aj bez konektivity na internet. Vo chvíli, keď naše zariadenie bude znovu v online režime, všetky nami vykonané zmeny budú automaticky zosynchronizované. Synchronizácia ponúka benefity, ktoré oceníme pri ukladaní príloh emailov alebo opačne, komfortné pridanie prílohy napr. z konkrétnej lokality v Teams, alebo zálohovanie pracovnej stanice.

Rozumiete M365?

Možno poznáte základné princípy, ale želanú efektivitu z používania aplikácii a práce v Microsoft 365 dosiahneme vtedy, ak si používatelia vzdelávaním a tréningom osvoja zaujímavé „fičurky“ a užitočné triky v tomto prostredí. Neváhajte nás osloviť – a my nájdeme spôsob ako vás vo firme kontinuálne rozvíjať v Microsoft 365.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR

Marcela Gottwaldová
marcela.gottwaldova@gamo.sk



Microsoft 365 predstavuje dynamiku. V Lunys ho využili naplno

Vzhľadom na dynamický rozvoj technológií a potrebu udržať krok s modernými pracovnými nástrojmi sa v spoločnosti Lunys rozhodli využiť potenciál Microsoft 365. S cieľom optimalizovať pracovné postupy a zabezpečiť bezproblémové využívanie nových funkcií a možností M365 investovali do vzdelávania svojich zamestnancov.

Vývoj moderných technológií prináša do firemného prostredia neustále výzvy a spoločnosť Lunys sa im nebráni. S investíciou do vzdelávania zamestnancov a implementáciou Microsoft 365 otvárajú dvere novým možnostiam spolupráce a efektivity v tímoch. Absolventi školenia zdieľajú svoje príbehy, pocity a skúsenosti, ukazujú, že modernizácia nie je len trendy, ale zároveň aj nevyhnutnosťou pre úspešné firmy.
Možno aj pre iné firmy sú tu jasné signály, že školenie poskytlo nielen praktické, ale aj inšpiratívne aspekty.

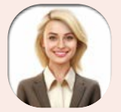
Spoločnosť Lunys, ktorá začala ako malý rodinný podnik, sa transformovala do stabilného a spoľahlivého obchodného partnera so silným záväzkom k moderným technológiám. Ich príbeh pokračuje a Microsoft 365 sa stal jedným z inovatívnych nástrojov na podporu ich úspechu. Inovácie a efektívne využívanie moderných technológií nie sú len trendom, ale nevyhnutnosťou pre firmy, ktoré sa chcú rozvíjať. Lunys sa stávajú príkladom toho, ako správne vzdelávanie a implementácia moderných nástrojov môžu posunúť podnikanie na vyššiu úroveň.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR

Martina Kormaník
martina.kormanik@gamo.sk

Pridajte sa k Lunys na ceste k inováciám a prosperite! V rámci ankety uverejňujeme skúsenosti a postrehy účastníkov z ich školenia:

Školenie vnímam ako adaptáciu na používanie služieb Microsoft 365, čo mi umožňuje pracovať intuitívne, a zároveň bezpečne.



Zlepšila som sa v organizácii stretnutí v Outlooku. Viem, kde hľadať, pozrieť, alebo ako pridať kalendár ďalších kolegov, ktorých potrebujem mať prítomných na schôdzke. Objavila som tiež nové možnosti filtrovania správ, ktoré prispievajú k ich lepšej prehľadnosti.

Aj keď väčšinu funkcií osobne nevyužívam, školenie bolo pre mňa zaujímavé a obohacujúce.

Osvojil som si princíp ako zdieľať dokumenty s kolegami podľa ich požiadaviek. Už neposielam prílohy, ale zdieľam link na dokument! Vytvoril som si tak s kolegami efektívny systém spolupráce.

Za mňa má jednoznačný prínos zdokonalenie sa v Microsoft Teams, v rámci školenia sme sa naučili využívať skupiny efektívnejšie a zdieľať veľké excelovské súbory. Vyžívaním úložiska OneDrive a intenzívnym používaním firemného chatu v Teams sme viac vzájomne informovaní a zostávame v priamom spojení.

Inšpirujeme študentov pre sebarealizáciu v IT

Smart Room For Everyone – SMARFE je spoločný projekt firmy GAMO so školami a študentmi, fanúšikmi IT, v Banskobystrickom kraji. Rozvíjame spoluprácu firma – škola – žiak.

Študentom dávame príležitosť rozšíriť si digitálne zručnosti spolu s víziou inšpirujúcej realizácie sa v IT teraz aj po ukončení štúdia. SMARFE mení spôsob, akým sa technológie integrujú do vzdelávacieho procesu a pripravuje študentov pre technologickú budúcnosť. Ako? Pracujú na reálnych projektoch s využitím IoT technológií. Zúčastňujú sa workshopov na projektový manažment, bezpečnosť, rozvíjanie soft skills a komunikácie v IT praxi.

Do SMARFE sú aktívne zapojené Stredná odborná škola informačných technológií a 1. Súkromné Banskobystrické gymnázium. Pravidelne sa stretávame, hodnotíme priebeh projektu, diskutujeme so študentami o dôležitosti tém pre ich profesionálny rast.

Napríklad: V jednom zo zadaní projektu bola úloha vybudovať v rámci interaktívneho vyučovania „chytrú“ triedu na rôznych typoch škôl. Čiže: Prostredníctvom IoT senzorov zozbierať dáta a ich analýzou navrhnúť zlepšenie školských procesov, resp. praktického vyučovania predmetov zameraných na elektroniku a programovanie. Výsledok: Interaktívna komunikácia s hmatateľným benefitom.

Nadviazanie spolupráce so súkromnými firmami v oblasti IT umožňuje študentom získať praktické skúsenosti a rady od profesionálov, ktoré im otvoria dvere do profesií žiadaných na trhu.

Článok čítajte na platformofinvention.sk
klikni alebo oskenuj QR

Iveta Hlaváčová
iveta.hlavacova@gamo.sk

platform of invention

Informačné technológie pre podnikanie s nápadom

Vydavateľ
GAMO a. s.
www.gamo.sk

Sídlo redakcie
Kyjevské námestie 6
974 04 Banská Bystrica
redakcia@platformofinvention.sk
www.platformofinvention.sk

Grafická úprava a sadzba
Morse s. r. o.
www.morse.click

Spracovanie textov a štylistická úprava
TIME.is COMMUNICATION
www.time-is.eu

Spoznajte odpoveď na neproduktívnu administratívnu záťaž

Chcem zistiť viac

GAMO
INFORMAČNÉ TECHNOLÓGIE