Seznam.cz využívá výhod nástroje Syxsense Secure

Odvětví

- Poskytovatel internetových služeb – portál, katalogový server a vyhledávač.

Prostředí

- Více než 1500 interních uživatelů z nichž více než 1000 používá přístup VPN.
- Více než 10 externích dodavatelů s přístupem do sítě.
- 8 poboček.
- WIN OS (900), MAC OS, Linux.

Technologické potřeby

- Bylo nutné zavést spolehlivý systém ochrany, záplatování a monitoringu na koncových bodech.
- Bylo nutné snížit provozní náklady a zvýšit efektivitu.
- Hledala se náhrada nástroje MS SCCM.

Komponenty rešení

- Syxsense Secure

Výsledky a výhody

- Eliminace rizika zneužití hrozeb.
- Vytvořit plošný update trvá minuty namísto hodin.
- Lepší monitoring koncových bodů.
- Přívětivější uživatelské prostředí a intuitivní ovládání.
- Možnost využití vlastních dotazů.
- Centralizovaná správa z jedné obrazovky a automatizovaný monitoring.
- Snížení finančních rizik spojených s úspěšným útokem a s odstávkami.

SEZNAM.CZ

Vzhledem k velikosti prostředí klient vždy řešil zavedení nástroje pro zjednodušení aktualizačních procesů, zejména plošných update, které vyžadují časté zásahy do provozu a nelze se jim vyhnout. Pro tyto účely klient používal System Center Configuration Manager od výrobce Microsoft. Nástroj SCCM se však postupně neosvědčil jako správné řešení.

„I když nástroj SCCM provedl plošnou aktualizaci stanic, v centrální konzoli často nezobrazil všechny aktualizované koncové stanice. Obecně nám přišlo, že má systém z pohledu vizualizace a monitoringu významné mezery." popsal svou zkušenost Michal Malý, System Administrator ve společnosti Seznam.cz.

Svůj pohled na věc dodává také Jakub Štaubr, Techsupport Manager ve společnosti Seznam.cz.

„Podstatná nevýhoda SCCM je, že se na klienta může dostat jen přes zapnutou VPN bránu. To vytváří na uživatele zařízení další nároky a komplikuje práci všech účastníků, jak administrátora, tak i uživatele."

„Syxsense agent oproti tomu umožňuje přístup na klienta z centrální konzole bez vynuceného zapínání VPN brány na dané stanici. To je pro nás důležité." shrnuje tuto část problému Michal Malý.

Služby společnosti Seznam.cz jsou do značné míry založené na rychlosti a plynulosti jejich poskytování bez výpadku. Proto také IT tým hledal takové řešení, které umožní bezproblémové nasazení agenta s minimální zátěží na koncové body a k tomu poskytne spolehlivou cloudovou řídící jednotku.

Dohady ohledně použitelnosti SCCM zaměstnávaly celý tým IT dlouhodobě tak, že to přestávalo být únosné. V té době začal klient diskutovat o celém problému také v rámci pravidelných technologických konzultací s partnerem AMI Praha, který doporučil nástroj Syxsense jako vhodné řešení.

Již během testovacího provozu se ukázalo, že Syxsense naplní nejen potřeby klienta ale i předpoklady, které je schopen v takto rozsáhlém prostředí splnit pouze robustní enterprise nástroj. Kromě již zmiňovaného využití k monitoringu a aktualizaci všech koncových bodů, včetně serverů, uživatelé Syxsensu často oceňují také výborně zpracovanou historii provedených změn na každém zařízení.

To potvrzuje také Michal Malý.

„Již několikrát nám to usnadnilo hledání důležitých informací, např. datum nainstalovaných aktualizací nebo SW."

Jak se ukazuje i v mnoha jiných provozech, velmi důležitou součástí monitoringu koncových bodů je také bezpečnostní analýza zařízení. Syxsense pro tyto účely poskytuje robustní nástroj s funkcionalitou pokročilého skeneru zranitelností. Využití těchto funkcí je dnes pro klienta stěžejní.

„Odhalování a následná oprava bezpečnostních hrozeb jsou v Syxsensu skvěle zpracované. Hrozba jde většinou automaticky opravit, případně je k dispozici podrobný návod jak mitigovat. Asi úplně nejlepší je vytváření vlastních query nad stanicemi. Hlavně je hodně intuitivní a opravdu pomáhá." doplňuje opět Michal Malý.

Nástroj Syxsense Secure pomáhá dennodenně řešit provozní a bezpečnostní úkoly velmi efektivně a je hlavně určen pro administrátory a technické pracovníky, jejichž náplní práce je celkový monitoring aktualizací a hrozeb na koncových bodech. Jeho nasazení v provozu jednoznačně snižuje nepříjemné stížnosti bezpečnostního oddělení, což je vzhledem k jejich odpovědnosti pochopitelné a v mnoha velkých společnostech na denním pořádku.

„Díky Syxsensu máme nyní v týmu lepší pracovní atmosféru." zdůrazňuje Jakub Štaubr.

„Navíc, díky lepšímu přehledu o stavu koncových stanic můžeme nyní lépe plánovat investice do nového HW." dodává na závěr Michal Malý.

Od počáteční implementace systému Syxsense Secure a nastavení jeho parametrů byl klientovi k ruce, jako odborný partner, MSSP tým FreeDivision. V rámci svých služeb poskytuje FreeDivision uživateli vždy pravidelné konzultace po celou dobu užívání a podporuje jeho požadavky na budoucí vylepšení nástroje vzhledem k svému těsnému vztahu s výrobcem. V tomto případě FreeDivision poskytl uživateli své zkušenosti již vícekrát, np. v souvislosti s nastavením reportingu, u nějž nyní uživatel velmi oceňuje oddělený přehled o starších nahrazených a nových nahrazujících záplatách.

Syxsense – výrobce

Společnost Syxsense Inc. založena v roce 2012 se sídlem v Newport Beach v Kalifornii je celosvětový lídr v oblasti jednotné správy koncových bodů a jejich zabezpečení. Výrobce je předním poskytovatelem inovativní cloudové technologie, která poskytuje hlubokou viditelnost s detaily o každém koncovém zařízení, na každém místě, všude uvnitř i vně sítě a také v cloudu. Technologie kombinuje sílu umělé inteligence s odbornými znalostmi v oboru a umožňuje spravovat a zabezpečovat koncové body tím, že včas zabrání zneužití hrozeb, nebo je alespoň ihned zneutralizuje. Nyní již s více než 500 dlouhodobými enterprise zákazníky s počtem koncových bodů od 100 do 100 000 poskytuje různá řešení pro organizace všech velikostí i pro poskytovatele služeb (MSP). Značka Syxsense je synonymem prvního poskytovatele bezpečnostních IT řešení na světě, který nabízí správu záplat, skenování zranitelností a zabezpečení koncových bodů včetně mobilních zařízení v jediné konzoli.
Více informací naleznete na www.syxsense.cz

FreeDivision – poskytovatel implementace a služeb (MSSP)

FreeDivision je přední společností v oblasti řešení a služeb kybernetické bezpečnosti na trhu. Již více než 20 let působí úspěšně v oboru kybernetické bezpečnosti. Na českém a slovenském trhu zastupuje několik celosvětově uznávaných výrobců, jejichž řešení přináší exkluzivně spolu s týmem vyškolených odborníků a konzultačními službami. Portfolio společnosti v současné době řeší technické požadavky na splnění podmínek vyžadovaných zákonem o kybernetické bezpečnosti, normami ISO 27001, PCI DSS, NIS2, HIPAA, GDPR a eIDAS.
Více informací naleznete na www.freedivision.com

AMI Praha – dodavatel

Na trhu působí jako systémový integrátor již více než 27 let v segmentu ICT bezpečnosti, se specializací na autentizačně/autorizační procesy a řízení přístupů k informacím, bez ohledu na to, zda jsou přístupné na sdíleném nebo lokálním úložišti, či v podobě strukturovaných dat v informačním systému. Svým klientům poskytuje profesionální služby a individuální přístup. Společně s nimi se vždy snaží nalézt vysoce použitelná, efektivní a funkční řešení, která zjednodušují práci, snižují náklady a zvyšují bezpečnost a zisk. Její dlouhodobé výsledky potvrzují desítky spokojených klientů a řada prestižních ocenění.
Více informací naleznete na www.ami.cz

FREEDIVISION

Provozovna a korespondenční adresa
Rektorská 50/52
108 00 Praha 10 – Malešice
Česká republika

www.freedivision.com
+420 220 972 426