Případovka

AUTOCONT

Bezpečná a intuitivní správa firemní sítě i práv uživatelů z cloudu pro LetsGetChecked

ZÁKAZNÍK STRUČNĚ

Společnost LetsGetChecked především testuje osobní zdraví, kdy na základě provedených testů v domácím prostředí klienta provede zdravotní screening a ten tak získá díky jednoduché a výkonné technologii větší kontrolu nad osobním zdravím. Firma působí z center v USA, Kanadě, Irsku a ČR, provozuje veškeré firemní aplikace v cloudu.

LetsGet Checked

OBDOBÍ REALIZACE

únor - květen 2019

„Vzhledem k našemu prudkému růstu a nutnosti správy citlivých osobních údajů našich zákazníků z několika pracovišť, jsme potřebovali rychlé řešení, které by využívalo již zaběhlé systémy jako G-Suite. Navržené řešení splňuje všechny naše požadavky a směrnice, ať už GDPR v EU, tak HIPAA v Severní Americe."

Michal Tesař, Chief Technology Officer LetsGetChecked, PrivaPath Diagnostics Inc.

Výchozí situace a cíle projektu

Cílem společnosti bylo vytvořit bezpečné prostředí, ve kterém je přístup k citlivým zákaznickým údajům řízen centrálně. A současně s tím maximalizovat bezpečnost těchto dat prostřednictvím efektivní správy uživatelů, údržby koncových stanic a firemní sítě. Vyžadováno bylo splnit bezpečnostní směrnice regulující zacházení s citlivými osobními údaji v Evropě i Severní Americe.

Veškeré informační systémy společnosti jsou uživatelům poskytovány z prostředí privátního cloudu v Amazon Web Services. Požadováno bylo využití pouze cloudových služeb, bez nutnosti mít jakékoli lokální servery a aplikace.

PŘÍNOSY

- efektivní správa firemní sítě jediným webovým administračním rozhraním založená na cloudu
- přehledný monitoring datového provozu plošně přes celou firemní síť
- velmi snadné VPN připojení všech poboček do firemní sítě, čímž lze snadno navázat spojení s každou lokalitou
- stejně snadné VPN spojení poboček napřímo s prostředím privátního cloudu (vPC) v AWS
- vzdálená správa uživatelských profilů a jejich oprávnění na všech koncových stanicích
- zajištění aktuálnosti veškerého instalovaného softwaru a selektivního výběru instalovaných aktualizací
- možnost vzdálené správy operačních systémů Windows, Linux a MacOS
- snadný způsob řízení přístupu k periferním zařízením
- zajištění bezpečnosti dat v souladu se směrnicemi v EU i Severní Americe

POUŽITÉ TECHNOLOGIE

Cisco Meraki

JumpCloud

Sophos Central

Automox

Popis řešení

AUTOCONT tedy musel najít velmi progresivní řešení. Ve spolupráci se zákazníkem provedl analýzu a Proof of Concept celého řešení. Jako základ moderní síťové infrastruktury byla zvolena technologie Cisco Meraki a navržen cílový koncept, umožňující kompletní vzdálenou správu sítě jednotným administračním rozhraním a silné zabezpečení koncových zařízení za využití výhradně cloudových služeb. Navrženo bylo propojení všech lokalit prostřednictvím automatických VPN tunelů pro zajištění možnosti přístupu každého uživatele do celé sítě dle daného oprávnění.

Využitím služby JumpCloud, jenž tvoří cloudový adresář, je možné sjednotit a hromadně spravovat profily uživatelů napříč různými službami (profily na Windows, GSuite, atd.). RADIUS servery jako služba v kombinaci s přístupovými body Cisco Meraki vytvořily kontrolovanou bezdrátovou síť, do které se uživatelé přihlašují prostřednictvím PEAP protokolu a 802.1x, a to stejným účtem, jaký mají v GSuite.

Zabezpečení koncových zařízení je věnována maximální pozornost. O celou tuto činnost se stará platforma Sophos Central, jenž poskytuje správu a zabezpečení, což zajistí aktivaci nového nastavení, odesílání upozornění a sdílení kontextových bezpečnostních informací.

Lze vytvářet jak skupiny uživatelů, tak skupiny koncových zařízení, na která se mohou aplikovat rozdílné bezpečnostní politiky. S instalací agenta na koncová zařízení je instalován nejen klasický antivir, ale také tzv. Intercept X, který využívá umělé inteligence a strojové učení pro detekci známých i neznámých hrozeb.

O údržbu stanic, jejich patch management se stará Automox, který dokáže centrálně řídit veškeré aktualizace operačních systémů, tak i softwaru třetích stran. Lze řídit vlastní úroveň automatizace správy aktualizací, vynucovat konfiguraci a vidět v centrální konzoli, která zařízení vyžadují pozornost. Je poskytována okamžitá viditelnost zranitelností a hrozeb podle jejich názvu, ale také podle tzv. CVE čísla.

Zajímavost reference

Zákazník používá firemní aplikace a infrastrukturu v cloudu (AWS, Google atd.), lokální infrastrukturu má pouze ve formě PC a sítových prvků. Řešení navržené společností AUTOCONT využívající technologie Cisco Meraki, JumpCloud, Sophos a další umožnilo pružnou dodávku, jednoduchou implementaci a vzdálenou správu v lokalitách Irska, USA a ČR. Vše je řízeno z cloudu a s vysokým stupněm zabezpečením přístupů k citlivým datům než v případě lokální infrastruktury.

Koncept řešení svoji flexibilitu prokázal i tím, že díky rozvoji firmy byly počty uživatelů těsně před dodávkou v New Yorku zdvojnásobeny a v Dublinu ztrojnásobeny a dosáhly úrovně 300 uživatelů. V Dublinu navíc přibyla další, původně neplánovaná pobočka.