



Výzva

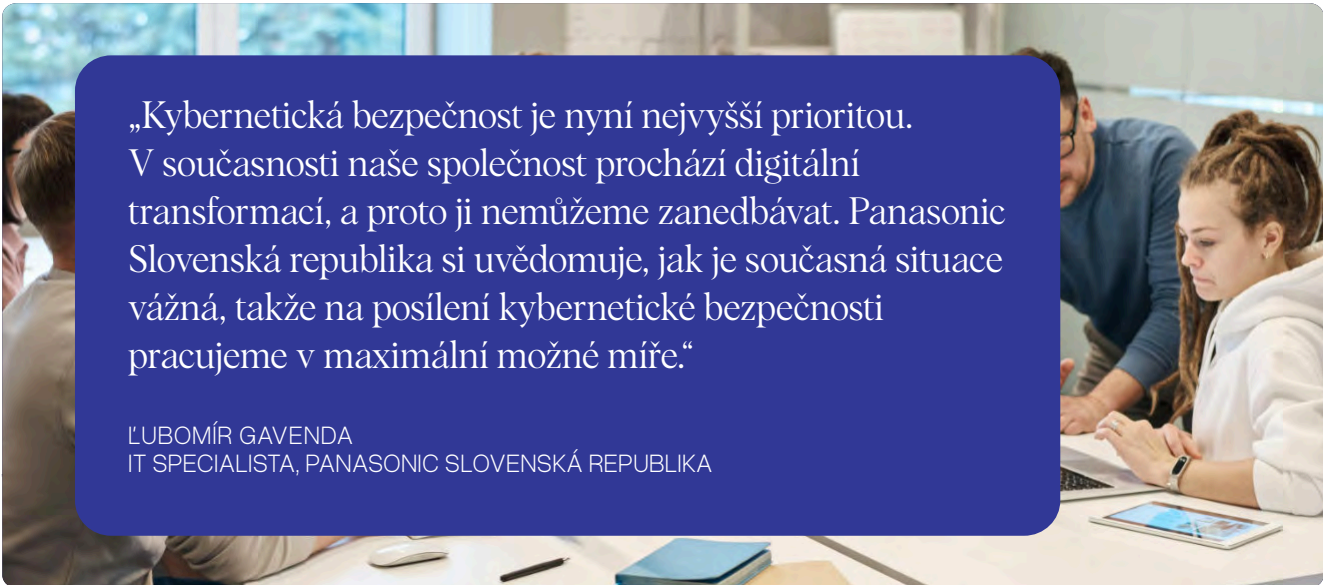
Předcházení pokročilým hrozbám

Cíle

Cílem IT týmu Panasonic Slovakia bylo implementovat ochranu proti zero day útokům a ochránit všechna zařízení včetně přenosných, typicky mobilních telefonů.

Výsledek

Výsledkem spolupráce byla rychlá a snadná implementace DNS zabezpečení včetně Home Office Security pro přenosná zařízení a tím i odstranění existujících slepých skvrn v bezpečnosti sítě.



„Kybernetická bezpečnost je nyní nejvyšší prioritou. V současnosti naše společnost prochází digitální transformací, a proto ji nemůžeme zanedbávat. Panasonic Slovenská republika si uvědomuje, jak je současná situace vážná, takže na posílení kybernetické bezpečnosti pracujeme v maximální možné míře.“

LUBOMÍR GAVENDA
IT SPECIALISTA, PANASONIC SLOVENSKÁ REPUBLIKA

Bezpečné prostředí je nutnou podmínkou výrazných a udržitelných inovací. To se týká i kybernetické bezpečnosti. Bez ní by inovativní firmy mohly přijít o důležité konkurenční výhody.

Proto se Panasonic Slovensko snaží být o krok napřed před hackery, protože jen tak může jejich výroba a výzkum fungovat bez narušení.

Organizace musí být stále ostražitě, protože nikdy nejsou zcela v bezpečí před hrozbami. Čím větší firmy jsou, tím vyšší je i pravděpodobnost, že se stanou terčem útoku.

Důvodů je více, například to, že si hackeři mohou od významnější oběti slibovat vyšší výkupné. Jindy zase mohou snít o větší reputaci a slávě.

„V dnešní době hraje kyberbezpečnost prim. Firewally už nestačí. Běžní uživatelé klikají prakticky na všechno, co jim přijde, takže je třeba implementovat řešení, které zajistí bezpečný provoz.“

LUBOMÍR GAVENDA
IT SPECIALISTA, PANASONIC
SLOVENSKÁ REPUBLIKA

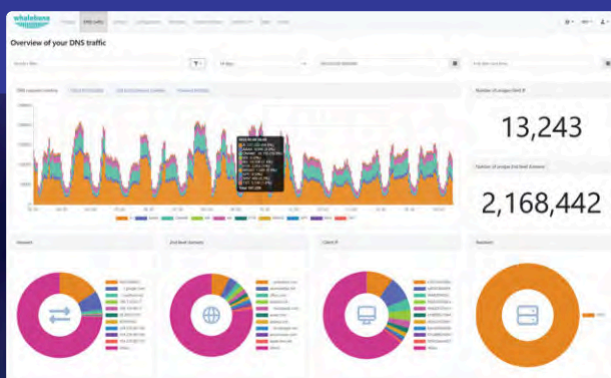
Řešení

Neprůstřelná bezpečnostní architektura

Firewally samy o sobě už dnes nestačí. Totéž platí pro kombinaci firewallu a antiviru. Už jen proto, že například na IoT zařízení nelze antivirus většinou vůbec nainstalovat. A co teprve přenosná zařízení, která zaměstnanci používají mimo kancelář?

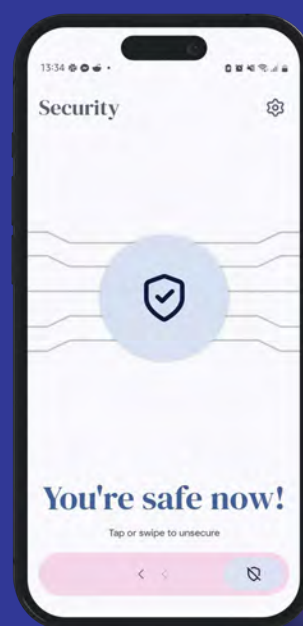
K vyřešení tohoto problému potřebujete snadno nasaditelné řešení, které dokáže rozpoznat dosud neviděné hrozby a zároveň chrání všechna zařízení bez ohledu na to, zda na ně můžete nainstalovat nějaký software nebo ne.

Whalebone Immunity všechny tyto požadavky splňuje. Ihned po nasazení začalo řešení blokovat škodlivou síťovou komunikaci, takže bezpečnostní tým společnosti Panasonic mohl okamžitě vnímat jeho přínos.



Implementace proběhla bezchybně, vše jsme zprovoznili během jediného dne. Zahrnovalo to tvorbu šesti nových virtuálních serverů, tři pro Immunity a tři pro nás. Vytvořili jsme resolvery, přes které teď běží veškerá komunikace.

LUBOMÍR GAVENDA
IT SPECIALISTA, PANASONIC SLOVENSKÁ REPUBLIKA



Výhody

Chráněno před neznámým

Whalebone Immunity se nasazuje s nulovým narušením uživatelské zkušenosti zaměstnanců. To znamená, že si uživatelé žádné změny nevšimnou až do okamžiku, kdy je některá jejich akce zablokována.

Nyní je infrastruktura společnosti Panasonic chráněna dosud chybějící bezpečnostní vrstvou, která je pro celkovou integritu sítě klíčová. Díky systému Home Office Security jsou chráněni i zaměstnanci pracující na dálku.



Dosud jsme neměli žádný systém, který by spolehlivě ochránil telefony nebo vzdálené počítače. Museli jsme se spoléhat na zabezpečení koncových bodů a sítě VPN. Proto jsme nasadili Whalebone Home Office Security, který teď tohle všechno pokrývá.

ĽUBOMÍR GAVENDA
IT SPECIALISTA, PANASONIC SLOVENSKÁ REPUBLIKA

DALŠÍ ZÁKAZNÍCI



Jednoduše přesměrujte traffic z vaší sítě na resolvery Whalebone a zahajte bezplatnou zkušební verzi.

immunity@whalebone.io

Rádi vám odpovíme na všechny otázky. Naším hlavním cílem je oboustranná spokojenost – uděláme vše pro to, abychom vám vyhověli.

www.whalebone.io

Více o našich produktech najdete na: whalebone.io/immunity

 Píče informací o DNS zabezpečení sledujte náš LinkedIn.