Případovka

AUTOCONT

Bezpečnostní dohled v Tescomě s.r.o.

ZÁKAZNÍK STRUČNĚ

TESCOMA s.r.o. je českým výrobcem originiálních kuchyňských potřeb, které navrhují a testují čeští designéři v Design centru ve Zlíně, kde také sídlí centrála společnosti. Řada výrobků TESCOMA nese označení světový patent a mnoho z nich získalo prestižní ocenění za design, jako jsou RED DOT DESIGN AWARD nebo German Design Award.

www.tescoma.cz

OBDOBÍ REALIZACE

4/2018

„Zařadili jsme do vlastní IT infrastruktury oči, ruce a hlavy profesionálů, kteří se kybernetickými hrozbami zabývají 24 hodin denně a jsou i v tento čas schopni řešit náš případný problém. Ba co víc, umí ho řešit ještě před tím, než nastane, protože se třeba vyskytl u některého z mnoha desítek jejich zákazníků. Jak bude fungovat služba v případě vážného incidentu, zatím nevíme, jelikož se zatím nic nestalo."

Michal Robek, IT ředitel společnosti Tescoma

Výchozí situace a cíle projektu

V kybernetickém prostoru se nachází mnoho nebezpečných útočníků, kteří jsou většinou absolutně neznámí. Náhodně nebo cíleně útočí na méně či více chráněné informační a komunikační systémy.

Tescoma v minulosti nedisponovala žádným systémem pro detekci bezpečnostních událostí a hrozeb a vzhledem k tomu poptávala komplexní řešení, u kterého by neměla potřebu udržovat tým správců, analytiků a bezpečnostních expertů na vysoké úrovni.

„Zajištění kybernetické bezpečnosti je nejdůležitější a zároveň navenek nejméně viditelný úkol IT manažera firmy. Cesty k jejímu zajištění vedou většinou přes nákup HW sond, vyhodnocovacího SW a také IT specialisty, který musí být neustále školen, protože nic se nerozvíjí rychleji, jako kybernetický zločin. Pořizovací a provozní náklady takového řešení jsou však neúměrně vysoké, tak jsme začali hledat řešení," dodal Michal Robek, IT ředitel společnosti Tescoma.

PŘÍNOSY

- Vysoká míra zabezpečení
- Přehled nad konkrétními bezpečnostními hrozbami s pohotovou reakcí v téměř reálném čase
- Efektivní řízení investice do budování kybernetické bezpečnosti, realizace formou průběžně placených služeb
- Vysoká odbornost, zkušenost i přehled v oblasti kybernetických hrozeb díky externímu, vysoce kvalifikovanému týmu specialistů

POUŽITÉ TECHNOLOGIE

AT&T Cybersecurity, USM appliance

Dell EMC PowerEdge server

Virtualizace Microsoft Hyper-V

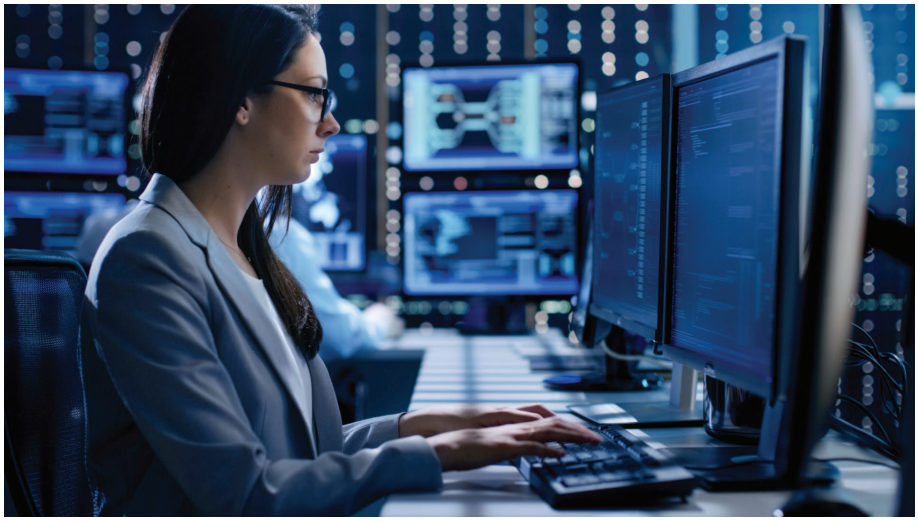
Služby „Bezpečnostního dohledu“ AUTOCONTu jsou založeny na co nejrychlejší detekci případného průlomu do informačního systému a zjištění jeho původu, cesty, rozsahu zasažení a pojmenování dopadu a následné správně řízené reakci a rychlé nápravě.

Popis řešení

Tescoma kvůli neustále rostoucímu kybernetickému nebezpečí hledala řešení, které umožňuje co nejpohotovější odhalení případného incidentu. Bezpečnostní dohled urychluje nejen detekci narušení, ale také určí původ incidentu, jeho možný dopad a rozsah, a tak díky zjištěným informacím je možné urychlit nápravu a obnovit důvěryhodnost IT zdrojů firmy.

Ideální variantou pro Tescomu bylo zavedení externí služby „Pokročilého bezpečnostního dohledu“ AUTOCONTu.

Pokročilý bezpečnostní dohled byl ještě rozšířen o službu Whalebone, která umožňuje pokročilou ochranu proti malware, za pomocí kontroly DNS dotazů. Kontrola na úrovni DNS překladu přináší mnoho možností za nízkou cenu. Kromě detekce umožňuje DNS filtrace i přímočarou a transparentní blokaci závadného provozu. Nasazení kontroly DNS provozu může proběhnout řízeně, po konkrétních částech sítě a jeho principy jsou transparentní pro všechny správce sítí. Přímo DNS protokol zvládne vyřešit případné problémy s dostupností překladačů.



Tescoma je napojena jako každý ze zákazníků na „federační server“ umístěný v prostředí AUTOCONT Security Operations Center (AC SOC). Všechny generované Kybernetické bezpečnostní události, alerty a incidenty jsou na tento server bezpečnou cestou replikovány. Bezpečnostní team má tak celkový přehled o všech dohledovaných zákaznících a dokáže tak včas a cíleně reagovat.