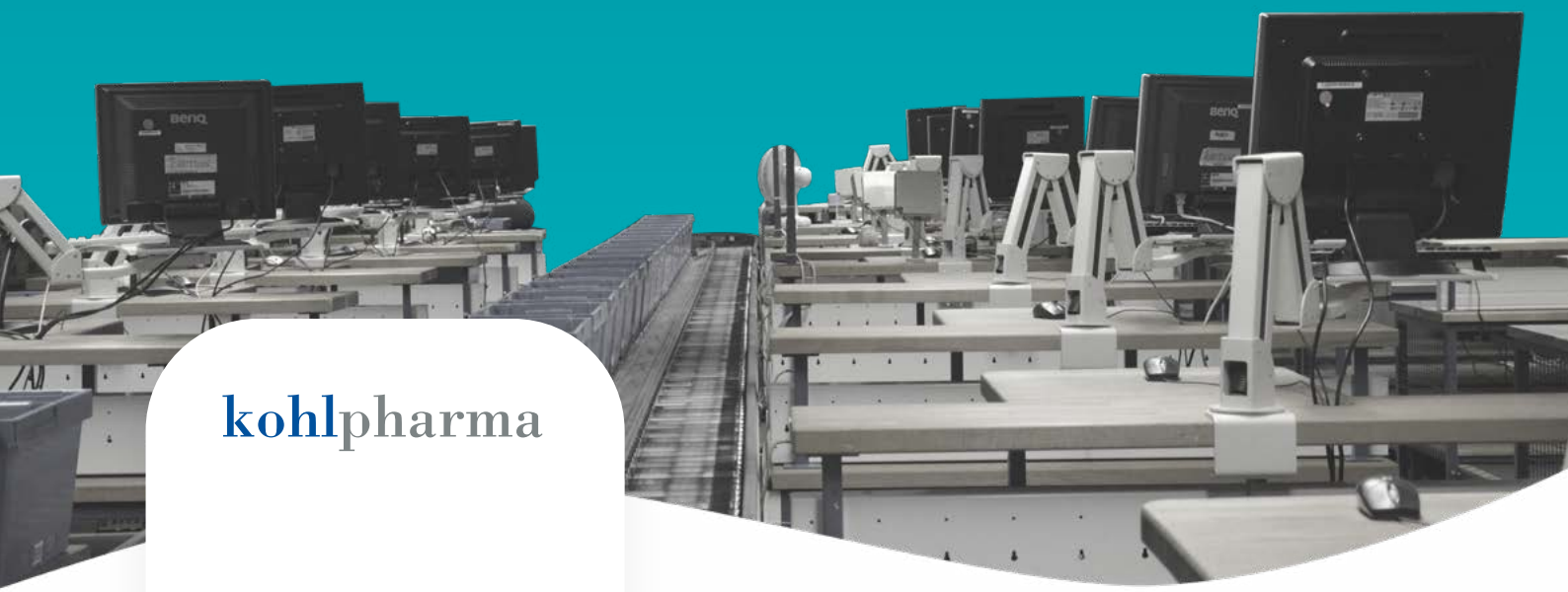
Prípadová štúdia

Zdravé IT, zdravá firma

Spoločnosť Kohlpharma ako významná firma v nemeckom farmaceutickom sektore vyžaduje prvotriedne zabezpečenie informácií. Cieľom firmy je zaistiť okamžitý prístup pacientov k liekom za rozumnú cenu, preto jej chod závisí od bezchybnej logistiky a spoľahlivej ochrany údajov, ktorú zabezpečujú **bezpečnostné riešenia ESET**.



kohlpharma

PRIEMYSELNÝ SEKTOR
Farmaceutická distribúcia

WEB
www.kohlpharma.com

KRAJINA
Nemecko

KONCOVÉ ZARIADENIA
1 250 endpointov

POSKYTOVANÉ RIEŠENIA A SLUŽBY

- ESET Enterprise Inspector
- ESET Dynamic Threat Defense
- ESET Endpoint Protection Advanced
- Služba Deployment and Upgrade
- Vstupná analýza a optimalizácia
- Služba ESET Technická podpora Premium

Prípadová štúdia/Kohlpharma

O SPOLOČNOSTI KOHLPHARMA

Kohlpharma bola založená v roku 1979 a v súčasnosti patrí medzi popredných dovozcov liekov v Európe. Táto spoločnosť so sídlom v sárskom meste Merzig nakupuje za priaznivé ceny originálne značkové lieky od renomovaných farmaceutických výrobcov z iných krajín EÚ a dováža ich do Nemecka. Pacientom a zdravotným poisťovniam tak prináša výraznú úsporu peňazí a pohodlie a aj lekári vďaka nej ušetria svoj rozpočet. Kohlpharma má 800 zamestnancov a dodáva kvalitné lieky pre lekárne, ako aj nemecké farmaceutické veľkoobchody.

KOMPLEXNÉ POŽIADAVKY

Kohlpharma je tiež lídrom v oblasti implementácie plnej automatizácie a Priemyslu 4.0 v Nemecku. Mnohé z jej kľúčových pracovných postupov už boli čiastočne alebo plne automatizované. Takéto systémy sú potenciálnymi cieľmi kybernetických útokov a vyžadujú komplexnú ochranu. Kohlpharma preto hľadala inovatívne IT bezpečnostné riešenie, ktoré by zahŕňalo nielen ochranu pred malvérom, ale aj systém detekcie a následnej reakcie na útoky na koncové zariadenia (EDR). Johannes Zenner, projektový manažér spoločnosti Kohlpharma, vypracoval ambiciózny súbor požiadaviek z ekonomického, funkčného a administratívneho hľadiska. Do užšieho výberu sa dostali iba traja poskytovatelia bezpečnostných riešení. *„ESET nám vrelo odporučil náš poskytovateľ počítačovej podpory, spoločnosť ttt-it AG. S veľmi dobrou mierou detekcie, najmodernejšími technológiami a odporúčaniami od spoločností Gartner a AV-Comparatives ESET dokonale spĺňal naše podmienky,"* spomína Johannes Zenner.

Kohlpharma podrobne preskúmala všetky potenciálne riešenia. Produktom ESET sa presvedčivo darilo v niekoľkých testovacích prostrediach s klonovanými servermi a koncovými zariadeniami z produkčného prostredia. *„Pomer medzi nákladmi na produkty ESET a ich prínosom bol výrazne lepší ako v prípade ostatných konkurentov. Presvedčili nás však dva netechnické faktory. K uzavretiu dohody prispela vysoká úroveň angažovanosti a otvorená komunikácia bez prázdnych sľubov,"* hovorí Stefan Pistorius, manažér pre správu a spracovanie elektronických údajov spoločnosti Kohlpharma.

SPUSTENIE V REKORDNOM ČASE

Trvalo iba šesť týždňov, kým sa podarilo úplne nasadiť balík riešení ESET Endpoint Protection Advanced, ktorý zahŕňa ESET Endpoint Security, ESET File Security a ESET Security Management Center. V ďalších dvoch fázach boli zavedené aj nástroje EDR ESET Dynamic Threat Defense a ESET Enterprise Inspector. *„Migrácia všetkých 1 250 zariadení na riešenia ESET sa vyznačovala vysokou mierou profesionality a harmonickou spoluprácou všetkých zúčastnených strán. Bol to ukážkový proces,"* hovorí Stephan Kapetanios zo spoločnosti ttt-it AG. ESET, ttt-it AG a Kohlpharma počas celého procesu migrácie úzko spolupracovali a vo veľmi krátkom čase sa im podarilo implementovať aj tie najšpecifickejšie nastavenia.

„Komplexné IT bezpečnostné riešenie musí správne fungovať a zároveň sa musí dať ľahko používať. ESET dosiahol túto rovnováhu ukážkovým spôsobom.“

Stefan Pistorius
Manažér pre správu a spracovanie elektronických údajov, Kohlpharma

HLAVNÉ VÝHODY

- Vysoká úroveň ochrany
- Jednoduchá implementácia
- Podrobné správy
- Nepretržité služby a podpora
- Efektívnosť nákladov

DOKONALÝ IT BEZPEČNOSTNÝ NÁSTROJ PRE KRITICKÚ INFRAŠTRUKTÚRU

„Spoločnosti klasifikované ako objekty kritickej infraštruktúry (KI), ako je aj tá naša, musia venovať oveľa viac pozornosti IT bezpečnosti. Preto sme do našej bezpečnostnej architektúry integrovali nástroj na detekciu a následnú reakciu na útoky na koncové zariadenia (EDR),“ hovorí Johannes Zenner. Znamená to, že do siete nemôže preniknúť žiadny malvér a všetky zraniteľnosti sú detegované. Keby sa logistika v dôsledku útoku zastavila, spoločnosti by to nepochybne spôsobilo finančné straty vo výške miliónov eur denne. Čo je však ešte horšie, podobná situácia by viedla k strate dôvery pacientov a firemných zákazníkov, ktorú si Kohlpharma tak starostlivo budovala. Takéto škody je veľmi ťažké napraviť. Preto sa Kohlpharma spolieha na tieto dve riešenia ESET – *ESET Dynamic Threat Defense a ESET Enterprise Inspector.*

ESET DYNAMIC THREAT DEFENSE: DODATOČNÁ OCHRANA PRED NOVOVZNIKNUTÝMI HROZBAMI

Siete sú každý deň vystavené stovkám neznámych súborov. Jednoduché dokumenty a iné nespustiteľné súbory zvyčajne nepredstavujú pre uznávané bezpečnostné riešenia problém. Úplná automatizácia procesov v spoločnosti Kohlpharma však spôsobila, že veľa spustiteľných súborov, napríklad súborov určených na aktualizáciu jednotlivých počítačov alebo zariadení, sa prenáša zvonku. To môže byť, samozrejme, veľmi nebezpečné, pretože .exe súbory môžu obsahovať skrytý malvér. Zároveň je spustenie súborov nevyhnutné pre bezproblémovú prevádzku. Riešením je spúšťať ich v izolovanom priestore (sandboxe), aby sa vyhodnotilo ich správanie. Takéto riešenie však nanešťastie vyžaduje veľa výpočtových zdrojov a rôzne šablóny sandboxu, a preto nie je možné ho aplikovať lokálne.

ESET Dynamic Threat Defense (EDTD) ponúka cloudový sandbox, ktorý dokáže identifikovať nové, doteraz neznáme hrozby. Týmto spôsobom dopĺňa nainštalované ESET produkty a pre koncové zariadenia spoločnosti Kohlpharma zabezpečuje ďalšiu vrstvu ochrany. Vzorky sa automaticky (v prípade potreby manuálne) odosielajú do ESET cloudu na analýzu. Jeho senzory rozširujú analýzu statického kódu o strojové učenie, kontrolu pamäte a analýzu správania. EDTD v porovnaní s bezpečnostnými riešeniami pre koncové zariadenia používa na detekciu potenciálne nebezpečných vzoriek oveľa širšiu škálu technológií. Výsledky cloudovej analýzy sa odošlú späť a všetky infikované súbory sú okamžite vyliečené alebo odstránené. EDTD navyše poskytuje správcom v spoločnosti Kohlpharma podrobné správy.

ESET ENTERPRISE INSPECTOR ODHAĽUJE VNÚTORNÉ ZRANITEĽNOSTI

Stefan Pistorius požadoval ešte širší prístup k IT bezpečnosti: *„Nestačí, aby sme na útoky reagovali pomocou klasických antimalvérových riešení. Chceme mať možnosť nezávisle odhaliť zraniteľnosti a odstrániť ich.“* Kohlpharma sa preto rozhodla pre ESET Enterprise Inspector. Tento nástroj na detekciu a následnú reakciu na útoky na koncové zariadenia (EDR) od spoločnosti ESET zhromažďuje údaje o akciách a udalostiach v pripojených koncových zariadeniach v reálnom čase a automaticky kontroluje, či údaje zodpovedajú kritériám podozrivej aktivity. Takto získané informácie sa spracúvajú a ukladajú v prehľadávateľnom formáte. Výsledná kompilácia neobvyklých a podozrivých aktivít umožňuje security špecialistom získať podrobnejšie informácie.

ESET Enterprise Inspector okrem toho poskytuje forenzné údaje o minulých incidentoch a ponúka usmernenia o možných protiopatreniach. Dokonca aj pokročilé pretrvávajúce hrozby (APT), ktoré už sú v sieti prítomné, sa dajú úspešne eliminovať. ESET Enterprise Inspector zhromažďuje a kombinuje komplexné informácie zo všetkých detekčných technológií ESET vrátane strojového učenia.

JEDNODUCHÁ SPRÁVA POMOCOU WEBOVÝCH KONZOL

Na prvý pohľad sa táto kombinácia mnohých rôznych produktov a technológií môže zdať komplikovaná. Johannes Zenner má však všetko pod kontrolou vďaka webovým konzolám, ktoré ESET poskytuje. Kľúčovým nástrojom je ESET Security Management Center, ktorý mu umožňuje centrálne spravovať všetky koncové zariadenia a servery. Používa tiež ešte jednu konzolu na správu produktu ESET Enterprise Inspector. *„Oba nástroje mi uľahčujú každodennú prácu. Sú prehľadné, štruktúrované, dobre fungujú a ponúkajú rôzne možnosti,“* hovorí projektový manažér. *„Synchronizácia údajov medzi dvoma konzolami prebieha automaticky, takže vždy mám k dispozícii aktuálne informácie. A ak narazím na akýkoľvek problém, môžem sa spoľahnúť na pravidelne aktualizovanú a rozsiahlu dokumentáciu.“*

Nasadením bezpečnostných riešení ESET povýšila Kohlpharma ochranu svojich systémov na úplne novú úroveň. Zásluhu na tom nemajú len technické aspekty riešenia. Rovnako dôležité sú aj niektoré netechnické faktory, najmä úzka spolupráca medzi zákazníkom, dodávateľom a poskytovateľom počítačovej podpory, ako aj komplexné a spoľahlivé služby a podpora. Kohlpharma vie, že teraz má po boku silného partnera, a to aj v prípade krízy.

PRÍPAD

Kohlpharma hľadala nové IT bezpečnostné riešenie, ktoré by spĺňalo požiadavky ochrany kritickej infraštruktúry. Okrem antimalvérovej ochrany bolo potrebné posilniť aj bezpečnostnú architektúru spoločnosti pomocou nástrojov na detekciu a následnú reakciu na útoky na koncové zariadenia.

RIEŠENIE

Kombinácia profesionálnych riešení ESET, konkrétne ESET Endpoint Protection Advanced (vrátane ESET Endpoint Security, ESET File Security a ESET Security Management Center), ESET Dynamic Threat Defense a ESET Enterprise Inspector, úspešne chráni komplexnú bezpečnostnú architektúru spoločnosti Kohlpharma pred hackermi a kybernetickými zločincami.

PRÍNOS

ESET poskytuje zosúladený systém komplexných IT bezpečnostných riešení. Spoľahlivo chráni pred útokmi zvonku a identifikuje podozrivé interné udalosti. Vynikajúca použiteľnosť konzol ESET správcom značne uľahčuje prácu.