



LOMMA KOMMUN ANVÄNDER E-POSTSKYDD FÖR ATT SKYDDA SIG MOT OKÄNDA HOT

Företag

Lomma kommun

Bransch:

Offentlig sektor

Land:

Sverige

Lösning från F-Secure:[F-Secure Cloud Protection
for Microsoft O365](#)

Lomma Kommun stärker sitt IT-skydd mot Zero Day-attacker, där bedragare utnyttjar okända sårbarheter, med F-Secures nya molnbaserade e-postskydd.

BEHOVET AV STÄRKT SKYDD MOT OKÄNDA HOT OCH ATT KUNNA HANTERA DET I MOLNET

I 11 år har Lomma Kommun med ca 1700 anställda, använt sig av olika klientskyddslösningar från F-Secure för att skydda kommunen mot olika typer av cyberattacker. För att öka skyddet mot riktade cyberhot, vilket traditionella virussydd har svårt att hantera, införde Lomma kommun häromåret F-Secures EDR-lösning (endpoint detection and response) - ett system som med automatiserade sensorer och maskininlärning analyserar användare och larmar om avvikande beteenden.

I början av 2020 utsattes Lomma kommun för en så kallad Zero Day-attack, i form av ett e-post med en länk (som mottagarna aktiverade) med skadlig kod som spred sig i IT-systemet genom att utnyttja okända sårbarheter i kommunens programvara. Attacken orsakade betydande skador som kostade både tid och pengar att reparera och återställa.

I ljuset av detta beslutade sig då kommunen, med IT- och servicechefen Patrik Flensburg i spetsen, att ytterligare stärka sitt IT-skydd, inte minst mot just Zero Day-attacker, som har blivit allt vanligare på senare år. Dessa kan, förutom att hanteringen och återställandet av dess faktiska skadeverkningar kostade pengar och tid, även resultera i att känsliga och värdefull data hamnar i orätta händer, om intrången inte upptäcks och åtgärdas i ett tidigt skede.

"Vi insåg att vi måste lägga på nya skyddslager på vårt befintliga klientskydd i takt med att hackarna ständigt utvecklar sina attackmetoder."

Efter att ha testat flera olika lösningar för att stärka Lomma kommuns klientskydd och smidigt kunna hantera det i molnet, föll valet på F-Secures nya molnbaserade och framtidsanpassade lösning Cloud Protection for Microsoft Office 365, som kommunen implementerade i augusti 2020. Den stärker kommunens skydd mot Zero Day-attacker samt stärker dess Office 365-skydd, de inbyggda skyddet i Office 365 i sig inte skyddar alla de ingredienser som användarna populärar den med.

Cloud Protection for Microsoft Office 365 kontrollerar automatiskt innehållet i alla de mail och länkar som skickas till de kommunanställdas mailadresser och flaggar för eventuella avvikelser som bryter mönstret. Varje del av mailen skannas av och systemet reagerar direkt om det t ex upptäcker en fil med skadligt beteende och placerar den i en sandbox-miljö - en virtuell miljö där osäkra objekt sätts i karantän och körs, för att avgöra hur de beter sig och om de är skadliga eller ska tillåtas släppas igenom. Systemet känner även av och reagerar på mail med eventuella nätfiske-beteenden, samt på hot med ransomware.

Fyra miljoner kontrollerade mail – bara under de första två månaderna

Sedan systemet infördes i augusti 2020 hade det, bara under de första två månaderna, skannat av hela fyra miljoner mail, varav 51 objekt och 104 webbadresser hade identifierats som osäkra och flaggats för. Systemet hade valt ut och placerat 626 händelser, såsom t ex mail, kalenderinbjudningar, upplagda kontakter, Outlook-grupper mm i sandbox-miljön, för att testas.

"Den nya lösningen har tydligt ökat effektiviteten i vårt arbete, vilket har besparat oss både pengar och tid. Innan fick vi ibland lägga tid på att hantera skadeverkningar och återställningar av skadliga mail, såsom t ex nätfiske- eller ransomware-mail, som användare hade öppnat. Nu har vi en helhetslösning som garanterar att inga skadliga mail tar sig in i systemet. Vetskapen om att vårt system kontrollerar alla mail innan de släpps igenom gör att jag numera kan sova gott om natten"

Patrik Flensburg,
IT and Service Manager, Lomma kommun

ABOUT F-SECURE

Nobody has better visibility into real-life cyber attacks than F-Secure. We're closing the gap between detection and response, utilizing the unmatched threat intelligence of hundreds of our industry's best technical consultants, millions of devices running our award-winning software, and ceaseless innovations in artificial intelligence. Top banks, airlines, and enterprises trust our commitment to beating the world's most potent threats.

Together with our network of the top channel partners and over 200 service providers, we're on a mission to make sure everyone has the enterprise-grade cyber security we all need. Founded in 1988, F-Secure is listed on the NASDAQ OMX Helsinki Ltd.

f-secure.com/business | twitter.com/fsecure | linkedin.com/f-secure

