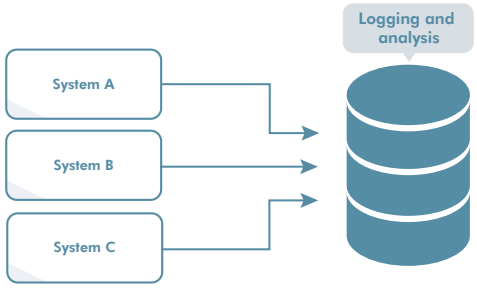
# Säker logginsamling med Splunk

Använder du Splunk för att samla in loggar? Vill du separera systemen för logginsamling från systemen som övervakas? Genom att placera en datadiod mellan Splunk Forwarder och Splunk HEC (HTTP Event Collector) säkerställer man att denna kommunikation är strikt enkelriktad och hindrar på så sätt den centrala logginsamlingen från att påverka de övervakade systemen.

Utmaning

## Säker överföring av logginformation

Splunk är en dataplattform för alla dina databehov. Den är byggd för kunder som har ett växande behov av datatillgång, kraftfull analys och automatisering. Splunk har idag många användare och används i många olika branscher. Splunk används ofta som en plattform för centraliserad insamling och analys av logghändelser. De system som övervakas, dvs skapar logghändelserna, är ofta känsliga i sig, eller innehåller känslig information.




**Figur 1.** Säker loggning med Splunk

Då man kopplar dessa system till ett system för logginsamling uppstår ett antal säkerhetsutmaningar:

1. Systemen kopplas samman via systemet för logginsamling, vilket gör att en incident eller attack mot ett av systemen kan sprida sig till de andra systemen via logginsamlingen.
2. En hotaktör som lyckas etablera sig i systemet för logginsamling kan därefter i nästa steg försöka attackera

de övervakade systemen.

3. Systemet för logginsamling och analys blir en måltavla för hotaktörer och riskerar att läcka information, samt exponerar de övervakade systemen för risker i form av bl.a. intrång och skadlig kod.

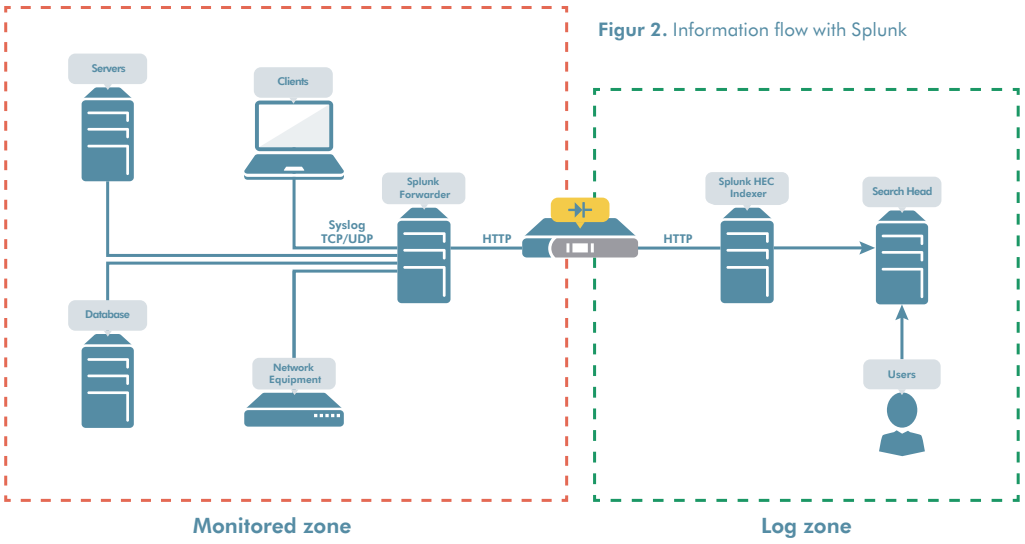
Vill man att en underleverantör, eller kanske bara en annan avdelning, ansvarar för insamling, lagring och analys av loggarna, t.ex. i form av en SOC (Security Operations Center) så blir det extra tydligt att man behöver skydda sina system mot intrång via logginsamlingen. Central logginsamling och analys är en mycket viktig del i en säker infrastruktur, men riskerar alltså att exponera systemen för nya potentiella attacker och incidenter.

Lösning

## Enkelriktat informationsflöde

När man använder Splunk för insamling av loggar skickas loggarna oftast först med protokollet Syslog till en Splunk Forwarder som skickar dessa vidare med över HTTP till en Splunk HEC (HTTP Event Collector) där loggarna lagras.

För att separera de övervakade systemen från systemen för logghantering placeras en datadiod mellan Splunk Forwarder och Splunk HEC Indexer (se Figur 2). På så sätt är du garanterad att inga incidenter i loggzonen kan sprida sig till de övervakade systemen samtidigt som logginsamlingen kan fortgå obehindrat.




**Figur 2.** Information flow with Splunk

Säkerheten bygger på att datadioden säkerställer ett enkelriktat trafikflöde från Splunk Forwarder till Splunk HEC Indexer.

Det faktum att trafiken endast tillåts flöda från den monitorerade zonen till loggzonen gör också att Splunk HEC Indexer inte kan signalera tillbaka till Splunk Forwarder om det inträffat ett fel eller om Splunk Forwarder tillfälligt behöver minska mängden loggar som skickas för att inte riskera att överlasta datadioden eller Splunk HEC Indexer. Detta kompenserar datadioden för genom att begränsa trafikflödet till ett konfigurerbart tröskelvärde. Om det överskrids resulterar det i att datadioden skickar ett HTTP 429 ”Too Many Requests” tillbaka till Splunk Forwarder som då minskar mängden loggar som skickas till datadioden. Datadioden kommer annars att svara med HTTP 200 OK tillbaka till Splunk Forwarder för att tala om att överföringen gick bra och sen skicka vidare HTTP-meddelandet till Splunk HEC Indexer.

Skulle det uppstå problem i kommunikationen mellan dioden och Splunk HEC Indexer kommer datadioden att försöka igen, ett konfigurerbart antal gånger, innan meddelandet kastas. En intern logghändelse skapas som talar om att det är problem med kommunikationen.

Fördelar

## En säker loggzon som uppfyller säkerhetskraven

Genom att använda en datadiod säkerställs att överföringen av data sker enkelriktat och det bidrar till en miljö som uppfyller högt ställda säkerhetskrav och rekommendationer. Lösningen eliminerar risken att en hotaktör attackerar de övervakade systemen från loggzonen. Du kan även känna dig trygg med att outsourca drift och ansvar för loggzonen till en underleverantör utan att denna får tillgång till de övervakade systemen.





advenica

Advenica tillhandahåller expertis, hög assurans och cybersäkerhetslösningar i världsklass för kritisk data-inmotion upp till Top Secret-klassning. Med oss stärker länder, myndigheter och företag informationssäkerheten och digitaliserar ansvarsfullt. Bolaget grundades 1993 och har EU-godkännande på högsta säkerhetsnivå. Våra unika produkter designas, utvecklas och tillverkas i Sverige.

**Läs mer på advenica.com**



ISO 9001 CERTIFIED
ISO 14001 CERTIFIED